System Wide Information Management (SWIM)

Final Program Requirements
Segment 2

June 23, 2010
Revision 10

Federal Aviation Administration
800 Independence Avenue SW
Washington, DC 20591

Approved by:_____ Date: _____
(Vice President, Operations Planning)

Submitted By:_____ Date: _____
(Director, Operations Planning, System Engineering)

Concurred By: _____ Date: _____
Ahmad Usmani, SWIM Program Manager

Concurred By: _____ Date: _____
Kimberly Gill, Manager, NAS Requirements
and Interface Management Systems Engineering

DOCUMENT CHANGE HISTORY

Version	Date	Description of Changes
8	8/31/09	Initial Segment 2 updates to Segment 1 FPR
9	10/7/09	Version 8 comment resolutions
10	6/23/10	Version 9 comment resolutions and editorial corrections

TABLE OF CONTENTS

1.0 BACKGROUND 1

1.1 Comparison of Segment 1 and Segment 2 2

1.2 Transition from Segment 1 to Segment 2 4

1.3 FPR Scope 5

2.0 OPERATIONAL CONCEPT 6

2.1.1 Overview 6
2.1.2 Programmatic Approach to SWIM Segments 9
2.1.3 SOA Implementation Approach 11
2.1.4 Segment 2 Organizational and Operational Impacts 12
2.1.4.1 Approach to Federating SOA Core Service 14
2.1.4.2 Approach to Federating SOA Governance 15
2.1.5 SOA Core Services Descriptions 16
2.1.6 SWIM Service Lifecycle Description 17
2.1.6.1 Design-Time (Development of Services) 17
2.1.6.2 Run-Time (Deployment of Services) 19
2.1.7 Governance 20
2.1.7.1 Quality of Service 21
2.1.7.2 Configuration Management 22
2.1.7.3 Enterprise Information Management 22
2.1.8 Information Security 23

2.2 Maintenance 26
2.2.1 Hardware Maintenance 26
2.2.2 Software Maintenance 26
2.2.3 Quantities and Locations 27
2.2.3.1 Segment 1 27
2.2.3.2 Segment 2 27
2.2.3.3 27
2.2.4 Schedule Constraints 28
2.2.4.1 Segment 1 28
2.2.4.2 Segment 2 29

3.0 TECHNICAL PERFORMANCE 29

3.1 Operational and Functional Requirements 29
3.1.1 Interaction Services 30
3.1.1.1 On-Demand NAS Portal 30
3.1.1.2 Administrative Portal 30
3.1.1.3 Browser - Reserved 30
3.1.1.4 Client - Reserved 30
3.1.1.5 Weather Notification - Reserved 30

3.1.1.6 Flow Constraint Notification - Reserved 30
3.1.1.7 Airport Status and Mission Critical Notification - Reserved 30
3.1.2 Mission Services - Reserved 30
3.1.3 Support Services 30
3.1.3.1 Data Access 30
3.1.3.2 Data Flow Management 31
3.1.4 SOA Core Services 31
3.1.4.1 Interface Management 31
3.1.4.2 Messaging Services 32
3.1.4.3 SWIM Security Services 34
3.1.4.4 SWIM Enterprise Services Management 36
3.1.4.5 Collaboration Services - Reserved 37
3.1.5 Technical Infrastructure Services 37
3.1.5.1 Boundary Protection 37
3.1.5.2 Information Systems Security Support Infrastructure 41
3.1.5.3 SOA Support Platforms 43
3.1.5.4 Web Application Hosting Capability 43
3.1.5.5 Data Storage 43
3.1.5.6 Computing Platform 43
3.1.5.7 Terrestrial Network Communication 43
3.1.5.8 Air/Ground Communications - Reserved 43
3.1.5.9 Sensor Systems - Reserved 44
3.1.6 Enterprise Governance 44
3.1.6.1 SOA Runtime Management 44
3.1.6.2 SOA Strategic Governance 45
3.1.7 Administrative Services 46
3.1.7.1 Data/Network Support Services 46
3.1.7.2 Services Provisioning Management 47

3.2 Product Characteristics and Performance Requirements 48
3.2.1 Reliability, Maintainability and Availability 48
3.2.2 Service Levels 48
3.2.3 Capacity 48
3.2.4 Recovery 48
3.2.5 Performance 49
3.2.6 Operational Software 49

4.0 PHYSICAL INTEGRATION 49

4.1 General 49

4.2 Real Property 49
4.2.1 Land 49
4.2.2 Space 49

4.3 Reserved 50

4.4 Environmental 50

4.5 Energy Conservation 50

4.6 Heating, Ventilation, Air Conditioning 50

4.7 Grounding, Bonding, Shielding, and Lighting Protection 50

4.8 Cables 50

4.9 Hazardous Materials 51

4.10 Power Systems and Commercial Power 51

4.11 Telecommunications 51

4.12 Special Considerations 51

5.0 FUNCTIONAL INTEGRATION 51

5.1 Integration with Other FAA Enterprise Architecture Elements 52

5.2 Information Requirements 52

5.3 Software Integration 52

5.4 Spectrum Management 52

5.5 Standardization 52

6.0 HUMAN INTEGRATION 53

6.1 Human Product Interface and Tasks 53

6.2 Employee Safety and Health 53

7.0 SECURITY 54

7.1 General requirements 54

7.2 Physical Security 54
7.2.1 Physical Security Monitoring 54

7.3 Information Systems Security 54
7.3.1 System Integrity 54
7.3.2 Availability 54
7.3.3 Access Control 54
7.3.4 Identification and Authentication 54
7.3.5 Confidentially 55
7.3.6 Non-Repudiation 55
7.3.7 Malicious Activity 55

7.3.8 Security Operations 55
7.3.9 Recovery 55
7.3.10 Security Management 55
7.3.11 Security Audit 55

7.4 Personnel Security 55

8.0 IN-SERVICE SUPPORT 55

8.2 Staffing 56

8.3 Supply Support 56

8.4 Support Equipment 56

8.5 Technical Data 56

8.6 Training and Training Support 57
8.6.1 System Training 57
8.6.2 Maintenance Training 57
8.6.3 Recurrent Training 57
8.6.4 Second Level Engineering Training 57

8.7 First and Second Level Repair 57

9.0 TEST AND EVALUATION 58

9.1 Critical Operational Issues 58

9.2 Test and Evaluation Requirements 58

10.0 IMPLEMENTATION AND TRANSITION 59

11.0 QUALITY ASSURANCE 59

11.1 Quality Program 59

11.2 Implementing Program Capabilities 59

11.3 SWIM Program Quality 60

12.0 CONFIGURATION MANAGEMENT 60

12.1 Configuration Management Program 60

12.2 Implementing Program Capabilities 60

12.3 SWIM Program Configuration Management 60

13.0 IN-SERVICE MANAGEMENT 61

13.1 Supply Support 61

13.2 Support Facilities 61

13.3 Training 61

13.4 First and Second Level Repair 61

13.5 Packaging, Handling, Storage, and Transportation (PHS&T) 62
13.5.1 Production Identification and Marking 62
13.5.2 Packaging & Transportation 62
13.5.3 Asset Identification – Bar Coding 62

13.6 Post Implementation Review 63

13.7 Service Monitoring 63

14.0 SYSTEM SAFETY MANAGEMENT 63

14.1 SWIM Safety Program 63

14.2 Implementing Program Capabilities 63

14.3 SWIM Program Safety 64

Appendix A – Mission Need Correlation Matrix……..A-1

Appendix B – Acronyms……..B-1

Appendix C - Overview of SWIM Segment 1 COI Capabilities……..……C-1

C.1.0 Flight and Flow Management COI…….C-1
C.1.1 En Route and TFM Interface……..……C-1
C.1.2 Terminal and TFM Interfaces…….……C-2
C.1.3 En Route and Terminal Interfaces……..……C-3
C.1.4 En Route and External User Interfaces…….…..C-3
C.1.5 TFM and External User Interfaces……..C-4

C.2.0 Aeronautical Information Management COI…….C-4
C.2.1 SUA Automated Data Exchange……..…….……..C-4

C.3.0 Weather COI…….……C-5

C.3.1. PIREP Data Publication……...C-5
C.3.2 Integrated Terminal Weather System (ITWS) Publication……..C-5
C.3.3 Corridor Integrated Weather System (CIWS) Publication……..C-6

Appendix D – Applicable Documents……..D-1

D.1.0 FAA/DOT Specifications, Standards, and Orders…….D-1
D.2.0 Other Publications and Specifications…….D-2

LIST OF FIGURES

Figure 1-1 Simplified SV-4b Services Functionality Description Mid-Term (NextGen 2018) 3
Figure 2-1 Point-to-Point Interfaces Transformed to SWIM 7
Figure 2-2 SWIM Conceptual Overview 8
Figure 2-3 SWIM Service Oriented Architecture 9
Figure 2-4 Segment 2 SOA Federation Concept 12
Figure 2-5 Development of Services 18
Figure 2-6 Registration of Services 19
Figure 2-7 Runtime Deployment of Services 20
Figure 2-8 High-Level EIM Methodology 23
Figure 2-9 SWIM ISS Conceptual Overview 25

LIST OF TABLES

Table 1-1 SV-4b Layer Descriptions 4
Table 2-1. SWIM Segment 1 Sites and Location 27

1.0 Background

Today's National Airspace System (NAS) comprises myriad systems developed over time for specific purposes. In general, they are connected discretely to support yesterday's decision making needs. Each of these interfaces is custom designed, developed, managed, and maintained individually at a significant cost to the Federal Aviation Administration (FAA). The Next Generation Air Transportation System (NextGen) relies upon a new decision construct that brings more data, systems, customers, and service providers into the process. Data will be needed at more places, for more purposes, in a timely manner, and in common formats and structures to ensure consistent use. The resulting decisions must then be distributed to the affected parties efficiently and reliably to support timely execution.

Based on these information needs, shortfalls were documented in the SWIM Mission Shortfall Statement (MSS), approved September 6, 2005 at the Investment Analysis Readiness Decision. The following provides an overview of the improvements that SWIM will provide in Segments 1 and 2 for each shortfall identified in the MSS. Appendix A provides traceability from the MSS to the SWIM Program technical requirements.

Costs to develop, test, deploy and support new interfaces and applications are too high. Costs of developing and maintaining custom point-to-point interfaces limits connectivity.

SWIM enables:

- Reusable, loosely coupled interfaces versus many point-to-point interfaces
- Reduced time and complexity for building new applications and interfacing existing applications
- Common shared services for information management replacing costly redundancies
- Information security controls to protect the information and systems using the SWIM information infrastructure

The NAS is not an agile air traffic system. The NAS is difficult to dynamically adapt to special events, disruptions and changing NAS user business models.

SWIM facilitates:

- Greater independence of geographical facilities and operations
- Easier and quicker system failure recovery
- Special events planning and implementation
- Automation and platform convergence consistent with the NAS Enterprise Architecture
- Enterprise-level business process definition, automation and management

Data sharing in the NAS is labor-intensive. Agility requires rapid, widespread and cost-effective dissemination of information. The current NAS infrastructure makes this cost prohibitive.

- SWIM provides the information infrastructure so that shared data can be published once and distributed electronically.
- SWIM provides standards, policies and processes as part of an Enterprise-level Governance framework
- SWIM provides technical mediation among SWIM stakeholders to ensure interoperability across systems implemented by different programs
- SWIM enables consistent information management across the enterprise

Timely access to common data is lacking in the NAS. A lack of shared situational awareness limits visibility into the current state of the NAS for NAS users and their customers.

- SWIM makes published data available to all authorized users
- SWIM enables enterprise-wide discovery of data and services
- SWIM provides advanced messaging capabilities to route data from authoritative sources to consumers as needed

The underlying tools to support becoming a performance–based organization are currently lacking. The information required to measure and monitor NAS performance is often not available; this limits the ability of the FAA to meet its goal to become a performance-based organization.

- SWIM provides the mechanism so that data can be mined for appropriate metrics.

1.1 Comparison of Segment 1 and Segment 2

SWIM Segment 1 established the first set of mission services supported by standard Information Technology (IT) infrastructure, standards and Governance processes. The mission services were proposed by members of specific Communities of Interest (COIs) and focused on incremental capabilities. In concert with the SWIM program, the Segment 1 COIs agreed these capabilities should be provided in a manner consistent with Service Oriented Architecture (SOA) objectives, SWIM priorities and COI programmatic considerations. SWIM provided significant guidance with respect to standards, policies and procedures and the SWIM Implementing Programs (SIPs) took responsibility for creating the mission services and implementing the SWIM-provided standard software comprising the core services. SWIM established applicable core service standards to ensure interoperability of the mission services and core services hosted by each SIP. Standards validation is an on-going activity among stakeholders using collaborative mechanisms such as the Architecture Working Group. The development and delivery of the core services and mission services was supported by SWIM implementation and Governance guidance and oversight activities. SWIM also took responsibility for establishing one centralized core service – the service registry – but the vast majority of the SWIM-funded functionality was developed, deployed and maintained by the SIPs with assets under their control.

SWIM Segment 2 requirements are being driven by NextGen concepts and plans for Operational Improvements (OIs) – that is, with a top-down approach unlike the bottom-up (COI) approach in Segment 1. Segment 1 capabilities continue to function in Segment 2, and in some cases are reused or repurposed to support segment 2 requirements. In

addition, many NextGen OIs driving Segment 2 requirements are transformational and provide far more complex and critical capabilities to support advanced, real-time Air Traffic Management (ATM) operations. There is a greater demand on, and need for, expanded capability in the Segment 2 core services compared to Segment 1. This results from an increased level of interactions across the SWIM IT infrastructure, in terms of message traffic intensity and data volume, and increased service and business process complexity and criticality in Segment 2.

Segment 2 includes additional capabilities to strengthen the overall NAS information system security posture. Security challenges have been documented in two reports: the *National Airspace System (NAS) Risk Analysis* and *Assessment Report* (RS Information Systems, 2007) and the report *A NAS Security Architecture* (MITRE, 2009).

Segment 2 is also leveraging the NAS Enterprise Architecture Framework (NASEAF) to specify SWIM capabilities and responsibilities consistent with an enterprise-level functional architecture. For example, the establishment and documentation of SWIM Segment 2 requirements is structured consistent with the Simplified SV-4b System Functionality Description for the Mid-Term. This artifact is depicted in Figure 1-1. Table 1-1 provides definitions of key components of the SV-4b and these terms are used in the remainder of this FPR. SWIM provides part of the NASEAF capabilities and other programs provide complementary capabilities.

Figure 1-1 Simplified SV-4b Services Functionality Description Mid-Term (NextGen 2018)

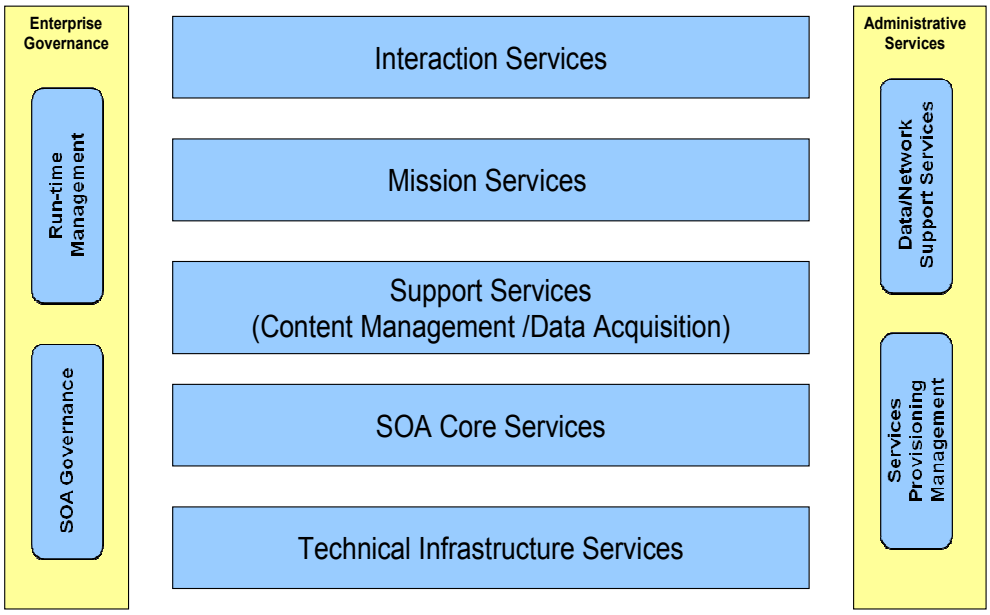


Table 1-1 SV-4b Layer Descriptions

Layer	Description
Interaction Services	Interaction Services provide human observation and interaction using state of the art display and keyboard. Purpose of Interaction service is to provide situation awareness and decision support. It often relies on information provided by the business logic of the Mission services and Support Services. Interaction service utilizes Browser and Client to access services which may be hosted remotely on Application servers and Portals on the NAS network.
Mission Services	The application services which provide mission business logic. They are residing in the NAS systems that support air traffic operations. Mission Service subscribes information provided by Support Services such as single authoritative source weather information or Flight and State Data.
Support Services	Data Logic supporting Mission Services. The logic exists at two levels: Data access to the persistent data required by the Mission Services and management of data flow to and between Mission Services. This logic is available to the mission applications as services and may be constructed with domain model semantics.
SOA Core Services	SOA Core Services layer primarily provides interfaces and interoperability to support the upper layers. The prime components are messaging services, collaboration services, security services, Interface Management and Enterprise Service Management.
Technical Infrastructure Services	This layer provides the hardware and software infrastructure to support day to day operations for all NAS services which are on the upper layers. Some components are the run-time computing platforms, data storage systems, network infrastructure, and enclave boundary and transport-level protection elements.
Enterprise Governance	This layer divides into Strategic Governance and Runtime Management. Strategic governance includes setting policy for strategy, services development lifecycle, runtime, and operations. Runtime Management is to administer runtime governance, auditing, and monitoring.
Administrative Services	Includes network and database administration services, Information Security Support services, and Incident Detection and Response services. Provides process and support services for Service provisioning management.

1.2 Transition from Segment 1 to Segment 2

The architectural approach for Segment 2 is expected to transition away from Segment 1's very limited amount of shared SOA Core Services. Specifically, in Segment 1, only the SWIM service registry/repository (implemented by SWIM) is provided as a shared

enterprise resource. All other SOA Core Services are implemented through SIP instantiations.

All Mission Services in Segment 1 are deployed by the SIPs. In Segment 2, resource sharing, especially SOA Core Services, increases through consolidation. Consolidation in Segment 2 means that SOA Core Services are developed, deployed and maintained by SWIM with assets under the control of the SWIM program. These SOA Core Services are provided to, and shared among, multiple NAS systems and programs. Segment 2 consolidation does not limit physical architecture alternatives (e.g., equipment locations) associated with distributed and centralized approaches.

The move to increase the level of SOA Core Services consolidation also opens the door to deploying certain other capabilities (e.g., Support Services and Mission Services) in a consolidated manner. Unlike Segment 1, the SWIM program does not envision explicitly defining the requirements for Segment 2 Mission Services. However, SWIM assumes new responsibilities for hosting all capabilities deployed to SWIM's consolidated infrastructure regardless of physical architecture. This includes all the normal responsibilities of a major NAS acquisition program.

The primary objective of SWIM's consolidated infrastructure is supporting enterprise-level interactions. That is, interactions among service consumers and service providers across the entire enterprise. These interactions result from the establishment and operation of Enterprise Services, i.e., any services that are exposed to, discovered by and used by systems in numerous organizational entities across the enterprise. Many Mission Services and Support Services are expected to be Enterprise Services in Segment 2. Note that the term "Enterprise Services" is not part of the SV-4b; it is a SWIM/SOA conceptual term that helps explain SWIM's role in providing the services in the SV-4b.

The Segment 2 architectural approach also allows additional SOA Core Services capabilities to be provided outside the consolidated infrastructure, in accordance with specialized needs of specific organizational entities. These capabilities support unique local requirements or requirements that extend or scale enterprise-level capabilities that cannot satisfy all local requirements. These capabilities supplementing consolidated SOA Core Services are established for use within an organizational entity consistent with those local requirements (e.g., to support unique SOA needs). Appropriate technical management responsibilities (e.g., Governance policies and procedures) are provided to ensure enterprise-level interoperability of all the SOA Core Services. Governance of Segment 2 capabilities is provided consistent with the allocation of elements of the functional architecture and maximizing interoperability and reuse.

1.3 FPR Scope

The SWIM FPR focuses on requirements allocated to the SWIM program. The Segment 2 requirements were derived from analyses of available NextGen planning documentation including descriptions of NextGen OIs. These analyses are defined and described in the SWIM Operation Services and Environment Definition (OSED) and include information on OIs and derived services that help drive the SWIM requirements and technical architecture to support the SWIM Segment 2 Final Investment Decision. This FPR provides Segment 2 requirements in addition to maintaining the legacy Segment 1

requirements. The document specifically tags Segment 2 requirements to delineate the Segment 1 and Segment 2 requirements. Each Segment 1 requirement also applies to Segment 2 unless it is marked "Segment 1 only." FPR requirements do not specify the allocation of the functionality to physical components of the NAS architecture.

2.0 Operational Concept

2.1 Operations

2.1.1 Overview

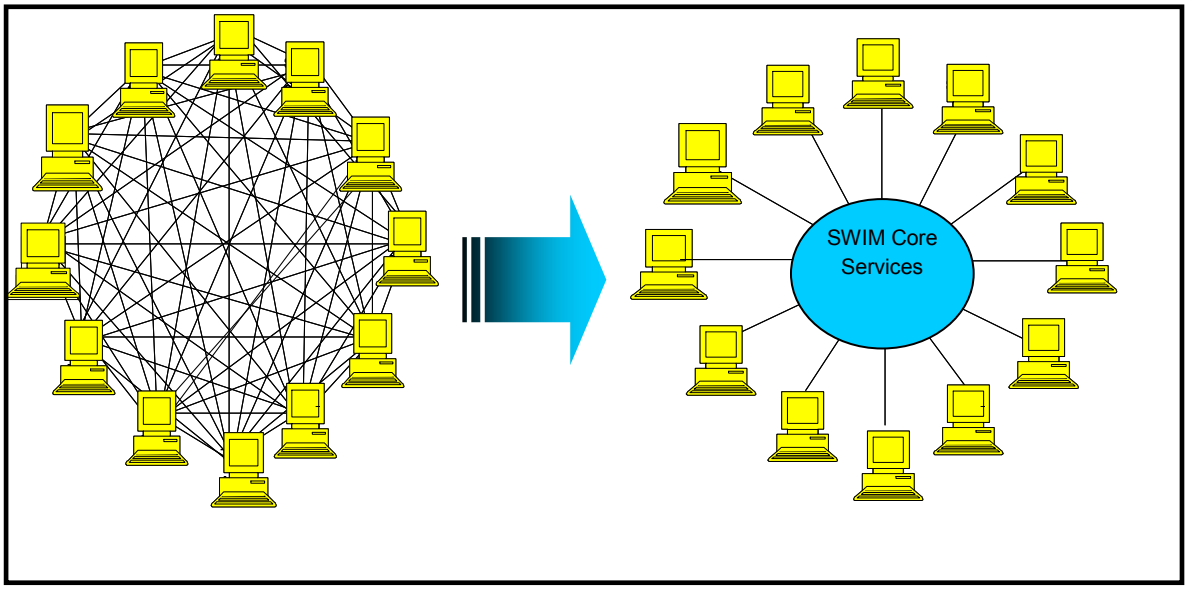
The FAA is a large producer, collector, consumer, and disseminator of information across the NAS and with partners outside the NAS. Because of the extent of the FAA's information activities, and the dependence of those activities upon stakeholder collaboration, the management of information resources is an issue of continuing importance.

The free flow of information within the NAS and between the FAA and its non-NAS partners is essential to NAS safety, capacity and efficiency. It is essential that the FAA minimize the cost of its information activities while maximizing information usefulness.

The operational concept for SWIM is to provide an open, flexible, modular, manageable, and secure information management and sharing architecture for any NAS operational data and other data exchanged among NAS and non-NAS service consumers and providers through SWIM information technology infrastructure. To achieve this concept, SWIM is to migrate NAS applications toward a loosely coupled (i.e., minimally interdependent), standards-based environment focused on information sharing (where loosely coupled systems tend to be highly modular with modules interacting through interface mechanisms that are independent of the modules). These open architecture principles provide value by reducing costs, reducing risks, enabling new services, and extending and therefore adding value to existing services.

The SWIM concept includes the ability to transform NAS application interfaces from a tightly coupled, point-to-point model into a SOA supporting loosely coupled services. This transformation is depicted in Figure 2-1. SWIM provides the flexibility to develop interfaces consistent with needs; it does not mandate a one-size-fits-all approach. The characteristics of each interface are determined based on the requirements and associated business case.

Figure 2-1 Point-to-Point Interfaces Transformed to SWIM



SWIM provides a set of SOA Core Services that facilitate development and execution of Mission Services and the migration of NAS systems to SOA-based applications. SWIM exposes an enterprise-level Mission Service (Information or Application Service) for Service Providers and makes information about that Service available to known and potential users through SWIM SOA Core Services. Service Consumers in turn use the SOA Core Services to locate and download information about the exposed services to consume and reuse the desired service. The stated concept is the cornerstone of SOA-based integration.

Figure 2-2 provides a conceptual overview of SWIM's role in providing standardized interfaces and information exchanges. SWIM sits atop the physical, network-level interface capabilities of the FTI IP Backbone. It provides message-oriented infrastructure, Interface Management and other Core Services that facilitate interoperability and reuse.

Figure 2-2 SWIM Conceptual Overview

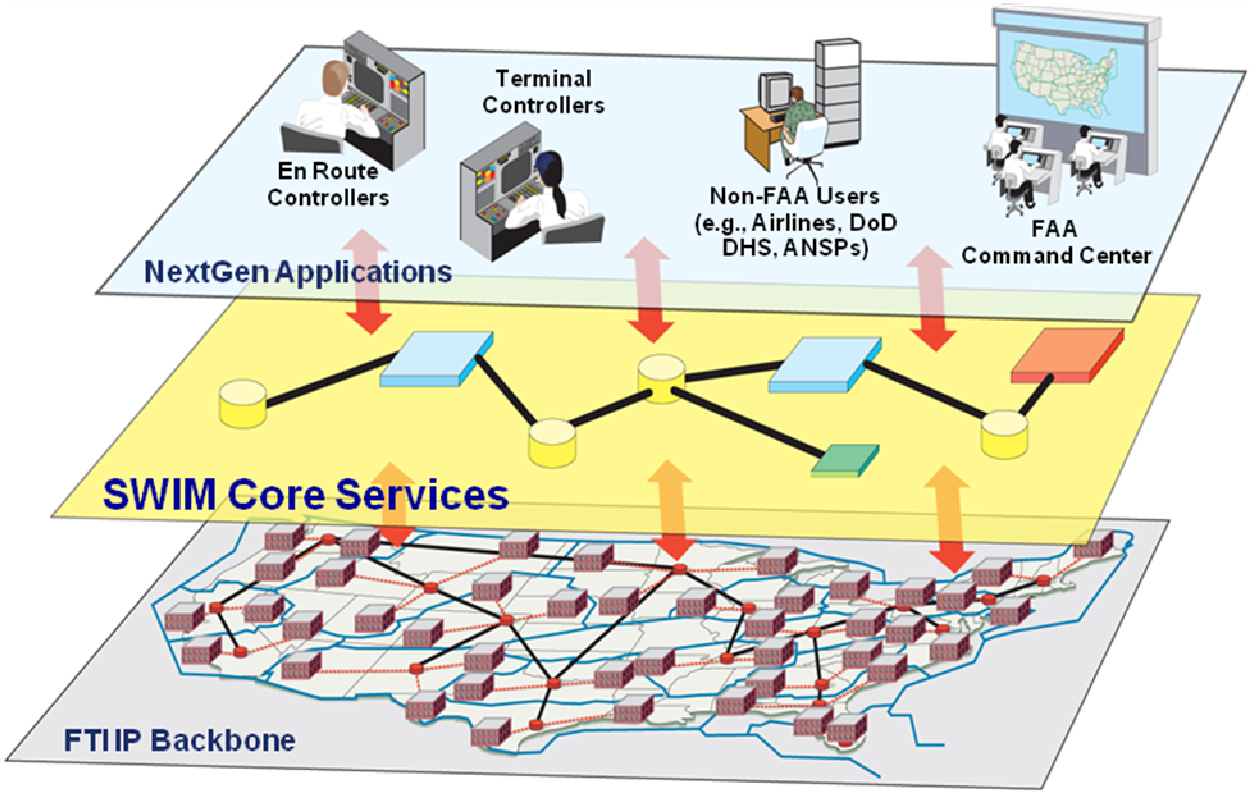
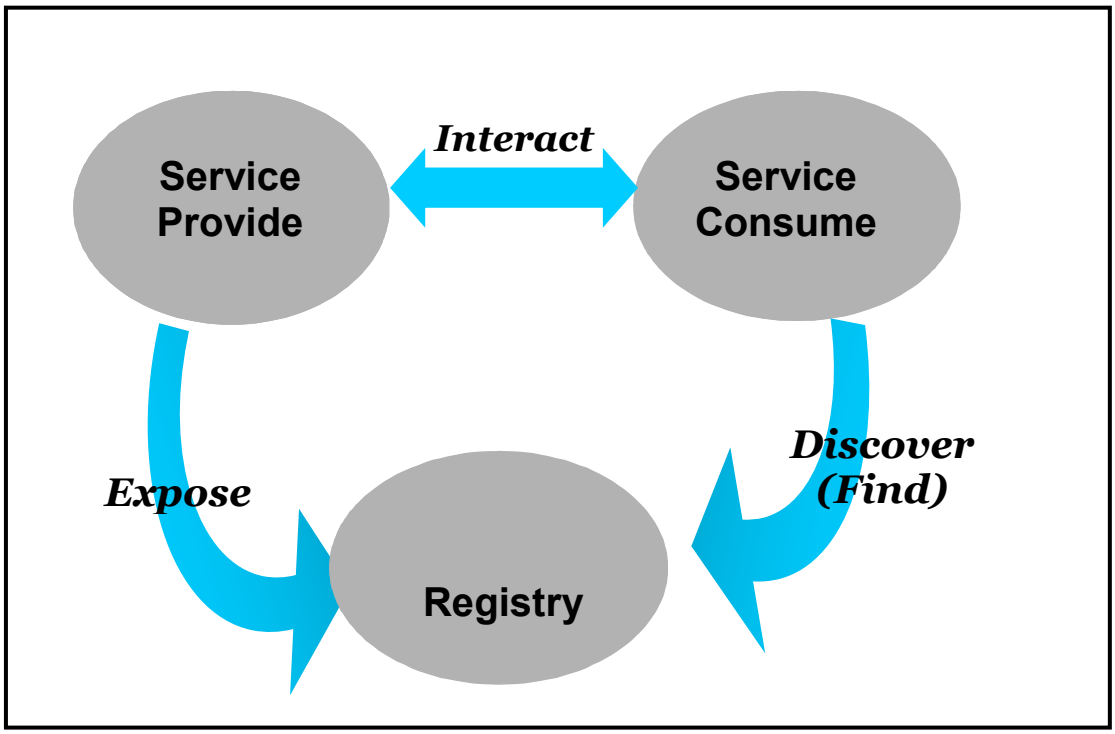


Figure 2-3 provides a top-level depiction of how the SOA service exposure and discovery activities, in concert with a service registry, can enable interactions between Service Providers and Service Consumers associated with NextGen applications. A Service Provider exposes a service that is ready for use by providing information to the Registry. For example, a web service implementation could expose the service using Web Service Description Language (WSDL). The registry provides capabilities enabling searches (e.g., by service category). A Service Consumer can use the Registry to find and discover the characteristics of a service

Figure 2-3 SWIM Service Oriented Architecture



2.1.2 Programmatic Approach to SWIM Segments

SWIM is being developed incrementally based upon the needs of various data communities, maturity of concepts of use, and segments that are right-sized to fit reasonable cost, schedule, and risk thresholds. Each Segment provides advances responsive to the SWIM MSS but each is intended to stand on its own with respect to costs and benefits. Although Segments build upon each other, each is approached and defined consistent with then-current conditions (e.g., with respect to budgets, schedules, technological advances and other factors) influencing Segment definition. In addition, the overall approach to defining requirements and selecting implementation and architectural approaches are subject to refinement Segment-to-Segment. The following compares and contrasts such concerns across Segments.

To define Segment 1, SWIM system engineers collaborated with NAS stakeholder groups (i.e., COIs) with the expertise to accurately describe how information is currently being used in the NAS, predict future NAS information needs, and discern how to best fulfill those needs using a net-centric solution. Segment 1 COIs include Aeronautical Information Management (AIM), Flight and Flow Management (F&FM), and Weather; others will form as needed over time. Segment 1 COIs identified nine capabilities for SWIM Segment 1 that decompose into Mission Services in a SOA environment. An overview of the Segment 1 capabilities by COI is included in Appendix C. Segment 2 Mission Services are being defined through analysis and decomposition of NextGen Operational Improvements. SOA Core Service capabilities for both SWIM Segments are defined and scaled to be consistent with the Mission Services in each Segment. Several

analyses, including a preliminary analysis of the OIs by the SWIM program, establish SWIM Segment 2 requirements, including the SOA Core Services required.

A Mission Service in Segment 1 is authorized for development with the allocated requirements through the SWIM program office and in the interest of the COIs. Service development is preceded by Service Providers and Service Consumers resolving requirements and architectural issues through COIs as necessary. Each party to SWIM interactions (e.g., Service Provider/Service Consumer), in any SWIM Segment, develops services according to SWIM Policy and Guidelines. In Segment 2, each service provider defines, provides investment analysis for, and acquires approval and funding for services as part of their standard acquisition mechanisms. This Segment 2 definition will also include significant collaboration among stakeholder communities. These collaborative bodies are expected to be similar in purpose to the COIs of Segment 1 but with a focus on defining Mission Services through more detailed decompositions of the NextGen OIs. The Segment 2 COIs will include several organizations and programs that contributed to Segment 1 COIs. There will also be additional participants, dictated by Agency plans and needs. For example the weather COI is expected to expand to include NNEW and selected weather consumers. In addition, participation is expected from the community of providers and consumers of NAS surveillance data. Collaboration with service consumers is used to help establish operational, functional and performance requirements. Collaboration with SWIM ensures appropriate IT infrastructure is specified to support the Mission Services. This collaboration begins during the concept development phase and continues through implementation of capabilities.

In Segment 1, when development of a Mission Service is completed, the service is deployed and monitored on a NAS System platform in the Run-time environment. During service execution, the approved platform provides service monitoring in accordance with the monitoring strategy for the hosting NAS System using SWIM provided Government Furnished Equipment (GFE) software (or a SIP-necessitated equivalent). Monitoring nominally includes the messages exchanged between the Service Provider and Service Consumer to capture and report any service execution anomalies. In Segment 2, the consolidated SOA infrastructure SWIM provides for Core Services is also a candidate platform for deployment of the Mission Services. Consideration is applied on a case-by-case basis for implementation of Mission Services as part of the consolidated SWIM infrastructure. This optional implementation approach may be advantageous in certain circumstances. Monitoring of Segment 2 Mission Services hosted on SWIM infrastructure platforms (if any) is a SWIM responsibility.

In Segment 1, rather than developing a fully separate infrastructure, the SWIM program provides GFE SOA Core Services software to the NAS programs developing the Segment 1 Mission Services. These programs, referred to as the SWIM Implementing Programs or SIPs (such as En Route Automation Modernization (ERAM), Traffic Flow Management System (TFMS), AIM, Corridor Integrated Weather System (CIWS), Weather Message Switching Center Replacement (WMSCR), and Integrated Terminal Weather System (ITWS) host the SOA Core Services software on their existing hardware, if available, or procure hardware as part of a planned future release. The SIPs provide configuration management, life cycle support, safety, and security for the SOA Core Services as part of their planned release upgrades, or as part of their new

acquisitions. Beyond the definition and furnishing of the interoperability-enabling standard SOA Core Services, SWIM provides policy guidance and Governance and manages the service registry that enables Mission Services to be described and discovered. For example, SWIM provides guidance in the form of a Qualified Vendors List that helps SIPs choose products (e.g., XML Gateway) that enhance interoperability.

Segment 2 includes additional Core Service capabilities and a more agile approach to the acquisition and management of the Core Services. Segment 2 moves toward more consolidation of SOA infrastructure, increasing the sharing of resources and therefore increasing the level of reuse. This is especially true with respect to the SOA Core Services that support enterprise-level interactions. Core Service consolidation increases overall NAS agility by enabling more efficient business process management and accommodation of change. Some core service capabilities continue to be implemented outside the consolidated infrastructure consistent with localized, or non-enterprise-level, needs. The SOA Governance responsibilities are allocated in a consistent manner. Segment 2 also provides increased information security capabilities consistent with enterprise-level information management. The following Subsections provide a more detailed description of concepts shaping the approach to SOA for Segment 2.

2.1.3 SOA Implementation Approach

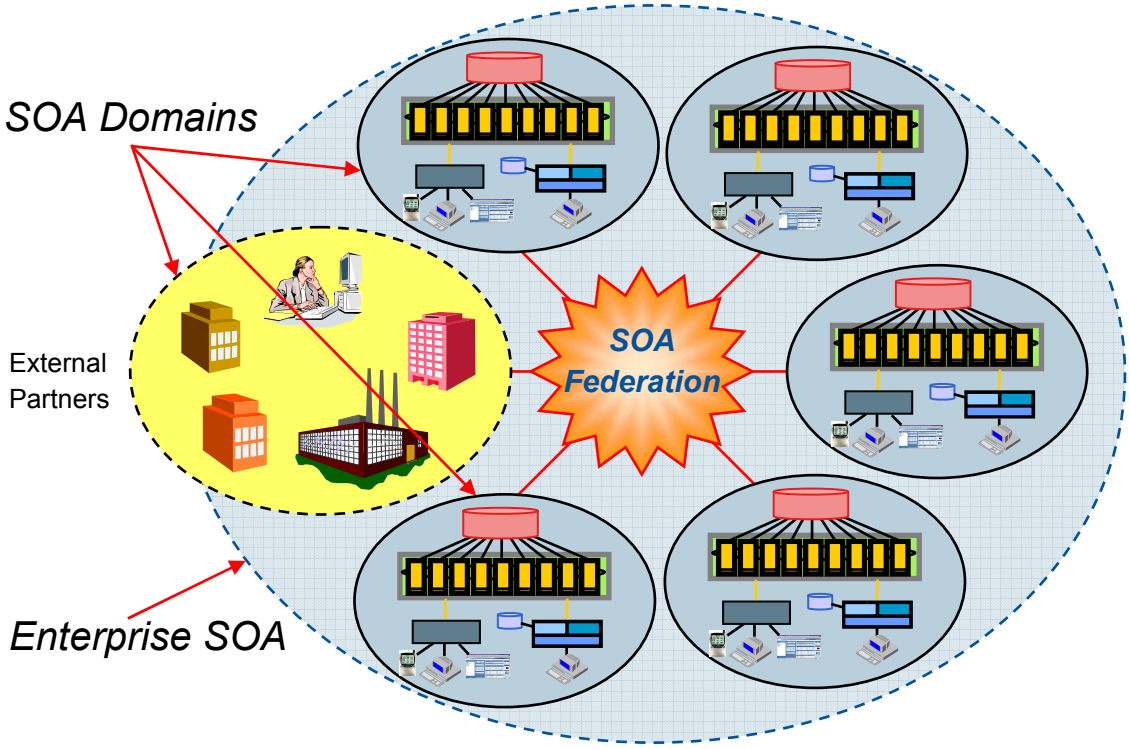
As mentioned above, the approach to SOA in Segment 2 leverages achievements in Segment 1 but also adopts new concepts and approaches to implementing SOA. The fundamental approach is based on establishing a federated SOA in the FAA. SOA federation is appropriate in large organizations comprised of semi-autonomous organizational entities and external partners. The intent of SOA federation is to facilitate adoption of enterprise-wide SOA by addressing political, organizational, and technical challenges that exist in large organizations like FAA. SOA Federation seeks a managed balance between two extremes: (1) autonomous and heterogeneous SOA development in each major program; and (2) a top-down imposition of uniformity across all NAS programs to maximize homogeneity across the enterprise.

The NAS prior to SWIM Segment 1 is structured closer to the heterogeneous model (1). Top-down homogeneity (2) has conceptual appeal but is impractical in large, well-established and diverse organizations like the FAA. SWIM Segment 1 makes significant progress toward a more collaborative and federated SOA for the NAS. But Segment 1 has limited scope for the SOA IT infrastructure elements and very limited scope for the Mission Services aligned with the new SOA infrastructure. SWIM Segment 2 significantly advances the trend toward collaborative and federated SOA consistent with greatly expanded Mission Services and supporting SOA infrastructure.

Segment 2 SOA federation is achieved by recognizing semi-independent SOA domains. A SOA domain is an appropriately scoped organizational entity that supports a number of related business processes with internal service providers and consumers. Nominally, each SOA domain has its own common business management and Governance authority, SOA infrastructure and Governance processes optimized to meet the functional requirements of its operational scope. Enterprise integration is achieved by integrating the SOA domains through SOA federation. SOA federation is defined by the set of

Enterprise Services, integration standards, and common infrastructure that are adopted to enable information sharing across SOA domains. SOA federation enables cross-domain sharing of services by providing appropriate interoperability infrastructure, enterprise-level Governance and mechanisms to enable necessary cross-domain collaboration. The flexibility afforded by SOA federation enables the most cost-effective migration to enterprise SOA given the size, complexity and organizational structure of the FAA. Figure 2-4 provides a notional depiction of how SOA domains are integrated through SOA federation [adapted from the Gartner presentation, "Accomplishing Enterprise SOA 'Mission Impossible' Through Federated SOA"]. The SOA Federation element includes the Core Services provided with SWIM's consolidated SOA infrastructure. SWIM Segment 2 focuses on providing the infrastructure and Governance required to achieve SOA federation.

Figure 2-4 Segment 2 SOA Federation Concept



2.1.4 Segment 2 Organizational and Operational Impacts

A central tenet of SOA federation is to allow individual SOA domains to tailor selected SOA infrastructure to fit their business needs and establish Governance processes to support their local SOA environment. SOA federation is achieved by applying appropriate SOA constructs at the enterprise level to enable interoperability and business process integration between the SOA domains. SWIM SOA federation requires a significant, enterprise-wide commitment to collaboration and consistent cross-domain Governance policies and procedures. To participate in a SOA federation, each SOA domain commits to give up some control over SOA IT infrastructure to an enterprise-level authority. The enterprise-level authority governs the common standards and

mechanisms that enable enterprise-wide interoperability. These commitments provide a counterweight to the domain-level autonomy allowed, facilitating enterprise-level coordination and an acceptable level of compliance. Consolidation of Core Services that support Enterprise Services simplifies both Core Service management and cross-domain integration. The separation of concerns inherent in this approach allows SOA domains to focus on their core missions by delegating responsibility for enterprise-level SOA infrastructure, thereby managing complexity while encouraging managed innovation.

The Segment 2 approach to SOA includes determining the levels of domain-level autonomy and enterprise-level control that are most appropriate for the organizational characteristics and business missions of the stakeholders. The transition from Segment 1 to Segment 2 includes making decisions concerning which elements of the SOA infrastructure are best provided at the enterprise level. SWIM stakeholders must decide which aspects of Governance and infrastructure are best managed by an enterprise authority and all aspects of responsibility must be allocated to organizational entities in the enterprise.

In adopting a federated approach to SOA, there is a need to identify and define SOA domains. SOA domains can be established to mirror organizational or geographic boundaries. For Segment 2, the SWIM approach to SOA federation recognizes the FAA's well-defined organizational boundaries (e.g., En Route, Terminal, Weather). In addition, several COIs that were formed to assist in shaping SWIM Segment 1 continue to be a factor in how SOA infrastructure is federated. However, Segment 2 SOA federation also recognizes that decisions about how to federate do not have to be based on existing organizational boundaries. For example, it may be advantageous to treat several FAA organizations as a single organizational element with respect to SOA infrastructure. This might be based on the need to share certain infrastructure elements to better enable business integration among them or to respond to unique challenges (e.g., with respect to security or performance characteristics).

An early and significant enterprise-level decision SWIM stakeholders collaboratively make is defining SOA domains. Existing FAA organizations and programs, in concert with SWIM, determine the criteria that help determine the best alignment of organizational elements with respect to SOA infrastructure. For example, these criteria help illuminate shared business interests where there is a need for a high degree of technical homogeneity in support of related business processes. Although a SOA domain can comprise any existing organizational entities, there is no need to reorganize the existing political or organizational structure. Nevertheless, it is necessary to establish collaborative bodies to make and manage technical infrastructure decisions affecting the stakeholders (e.g., organizational elements) in a SOA domain.

Segment 2 SOA domains are defined by examining existing organizational entities, their unique technical assets and plans, their common business interests, etc. in the context of the Enterprise Services and SOA infrastructure needed to support business objectives across the enterprise. Based on these assessments, enterprise-level needs and unique SOA domain needs are clarified. This information is used to define roles and responsibilities for SOA federation across the enterprise. The outcome of this activity is a consensus-based assignment of responsibility for each SOA infrastructure component and responsibility consistent with maintaining interoperability and business integration

among the SOA domains – and consequently the enterprise. SWIM SOA federation is applied to both the individual elements of the SOA interoperability middleware and SOA Governance. The following Subsections describe the Segment 2 approach to these aspects of SOA federation.

2.1.4.1 Approach to Federating SOA Core Service

A key consideration in implementing federated SOA is to ensure interoperability among the SOA domains – each of which can have (potentially different) interoperability middleware enabling intra-domain service providers and service consumers to share data and services. The SWIM term for these capabilities is Core Services and includes Messaging, Enterprise Service Management, Interface Management and Security. The SWIM concept provides the ability to treat intra-domain SOA needs differently than inter-domain (or enterprise-level) SOA needs. In the Segment 2 federated SOA, mechanisms are adopted to provide the bridges between any differing technologies (e.g., products and supported standards) implemented in different SOA domains that may impact enterprise-level interoperability. For Segment 2, SWIM provides a SOA domain focused on providing Core Services (and other selected interoperability middleware) required to support inter-domain (enterprise-level) interactions. SWIM provides mechanisms (e.g., Support Services) to bridge different SOA technologies and to bridge legacy non-SOA and SOA technologies.

This approach can be termed “third-party” because it provides a separation of concerns between the SOA IT infrastructure and the operational systems and programs that are focused on the FAA core missions (e.g., ATM). Since SWIM is not responsible for key operations like ATM (i.e., is neither a Mission Service provider nor consumer), it acts as a “third-party” provider of Core Services (and other supporting capabilities). This approach to providing cross-domain interoperability middleware clearly defines technical responsibility across the enterprise and allows the operational systems and programs to maintain focus on core FAA mission issues while SWIM coordinates SOA infrastructure issues across SOA domains. The third-party approach is most effective when the designated third-party is focused exclusively (or almost exclusively) on providing enterprise level SOA infrastructure and Governance to the other SOA domains. That scenario is most consistent with ensuring the separation of concerns that allows the other SOA domains to focus on their core capabilities supporting the FAA mission.

Given the number of different functions and technologies associated with Core Services, the third-party approach isn’t necessarily best in all cases. For example, the best approach to providing security across the enterprise may be markedly different from the best approach to providing messaging. In particular, even when a third-party approach is preferable, the third-party provider may be different for individual elements of Core Services. Each technology is considered on a case-by-case basis with a key factor being the way SOA domains are defined in the FAA. As mentioned earlier, collaborative analyses determine the best allocation of SOA capabilities to organizational entities. Those elements that are consistent with the third-party approach, and for which SWIM is the preferred third party, are incorporated in the SWIM consolidated infrastructure.

Certain elements of Segment 2 Core Services are most amenable to consolidation in the SWIM SOA domain. The consolidated capabilities focus on supporting Enterprise Services and cross-domain interactions while intra-domain SOA interactions are supported, as necessary, by specialized, domain-level capabilities. For example, federating the registry function involves using more than one registry – some dedicated to support significant intra-domain concerns plus a master registry at the consolidated enterprise level – and that can provide a hierarchical link to all other registries. The federation of messaging is conceptually similar: given the anticipated interactions within and among the SOA domains, the messaging functionality is federated consistent with intra-domain and inter-domain message traffic expectations. The adoption of Enterprise Service Bus (ESB) technology embodying several SOA functions can also be approached via federation similar to other components. Most elements of the ESB capability will be consolidated at the enterprise level but additional ESB capabilities can support unique domain-level needs. Examples of ESB capabilities include data transformation, routine and complex message routing, workflow management and service orchestration.

2.1.4.2 Approach to Federating SOA Governance

Each SOA domain provides Governance of its dedicated SOA infrastructure. In segment 2, the SWIM program provides a SOA domain focused on acquiring and managing the consolidated enterprise-level SOA infrastructure. In addition, SWIM provides the necessary enterprise-level Governance oversight to ensure interoperability of SOA elements federated among the other SOA domains. SWIM provides a mediation-based approach to enterprise-level Governance, including Governance roles, responsibilities and processes.

The mediation-oriented approach allocates overall SOA Governance to SWIM, leveraging its independence from the other SOA domains with respect to the enterprise mission. SWIM provides the collaborative leadership required but does not have any significant role in the business operations that could create bias, conflicts of interest or other counter-productive influences. SWIM's primary management role is to identify technology trends, help define technical evolution plans and lead efforts to reconcile technical differences among stakeholders (e.g., with respect to standards adoption) and help resolve associated management and process issues. Well-defined conflict resolution mechanisms (e.g., review boards), supported at the highest levels of the enterprise, enable contentious issues to be escalated and resolved.

Segment 1 stakeholder interactions are largely peer-oriented but SWIM is leading several important aspects of Governance including responsibility for the registry and defining enterprise-level governance policies and procedures. The mediation approach to Governance is consistent with agility. It leaves the current FAA organizational entities essentially unchanged but is more conducive to making changes as the NextGen plans unfold. The SWIM program will adjust its Governance role in accordance with evolving priorities and risks but existing FAA organizational entities (and SOA domains) are not expected to need to make major adjustments in their engagement model with SWIM mediation.

The mediation-oriented approach to Governance is consistent with the third-party approach to Core Services for enterprise interactions (provided as part of the consolidated infrastructure) and has similar advantages. SWIM Segment 2 naturally combines the third-party approach to Core Services and a mediation approach to Governance to achieve a federated SOA for the NAS.

2.1.5 SOA Core Services Descriptions

The following provides a top-level description of the SWIM SOA Core Services. The use of each specific SOA Core Service is dependent on the business needs for each Mission Service. Every service will not necessarily require every SOA Core Service or the same capability level. Core Services in Segment 1, implemented primarily by the SIPs, are provided in accordance with SWIM policies and standards. Core Services in Segment 2 include the legacy SIP implementations and, as described above, include additional functionality as part of the SWIM consolidated infrastructure and allows for federated SOA infrastructure as needed by SWIM stakeholders to support intra-domain requirements.

Four types of SOA Core Services are described below. SOA Core Services isolate IT concerns from business concerns, allowing developers to focus on applying service oriented principles to developing Mission Services without being distracted by IT issues. Core Services also promote re-use of existing Mission Services and the consolidated infrastructure. This generates cost savings, mitigates much of the integration technology risk, and provides a point of control for implementing enterprise guidance and integration patterns.

Interface Management includes capabilities that enable Service Providers to expose services and Service Consumers to discover services. It includes supporting capabilities such as management of service descriptions and data exchange requirements (typically, in a service registry) to assist in interface development. It also provides support for managing metadata such as the schemas that define the format and semantics of interface data elements. Interface Management capabilities provide consumers with information necessary to enable service discovery and execution without needing to know the details of the service connection path (e.g., endpoint location).

Messaging includes mechanisms supporting a variety of service invocation styles (e.g., publish-subscribe, request-response) and data exchange protocols. It includes the structures and metadata used in message routing and enables routing based upon the message payload or metadata. Messaging capabilities can include delivery allowing service consumers to receive queued messages after reconnecting to the network.

Security includes control mechanisms to enforce security policies at the service and message level including providing authorization-based access to data and services. Security controls are provided consistent with Federal Information Processing Standard (FIPS) Publication FIPS 199 information systems categories (i.e., low-impact, moderate-impact, or high-impact) and guidelines in National Institute of Standards and Technology (NIST) Special Publication 800-53 (as amended) to provide confidentiality, integrity, and availability. It ensures both Service Consumers and Service Providers can verify identities, validate digital credentials, authenticate themselves and assert access privileges

via authorization; and ensures confidentiality of information exchanged while invoking and consuming services. It protects information integrity, that is, guards against unauthorized modification of data and services. It also provides monitoring to detect and record information on specific events and actions. SWIM's SOA Core Services security is focused on service- and application-level interfaces and messages consistent with enterprise SOA principles. Capabilities are selected and implemented across the systems and organizations in the enterprise consistent with global and local security requirements and appropriate performance requirements.

Enterprise Service Management includes Governance and Monitoring. Governance manages services across all service lifecycle phases based on conformance to SWIM policies and procedures. Monitoring is how the NAS ensures the key requirements are met including the ability to capture, view, and report on service performance and usage. QoS and other performance metrics are defined and measured consistent with system and service requirements and address items such as throughput, reliability, availability, latency, response time, accuracy and fault data (e.g., for isolation and repair).

2.1.6 SWIM Service Lifecycle Description

The nature of how SWIM SOA Core Services are used depends on the mode of operation. SOA Core Services play a role in both development and execution of services. To clarify the discussion, two service lifecycle phases are defined: design-time and run-time. Design-time refers to the development activities preceding operational implementation of a service. Run-time refers to the activities during routine service operations.

The following provides a description of each service lifecycle phase, highlighting SWIM capabilities to help users create, expose, discover, manage, invoke and consume services. Distinctions between design-time and run-time capabilities are highlighted as needed. Governance policies and procedures play a significant role in many aspects of each service lifecycle phase. Selected Governance influences are mentioned in the next two subsections. The goal of the Governance policies and procedures is to promote designs and practices that result in services that are interoperable and re-useable. SWIM SOA Core Services provide critical SWIM functionality but Governance provides the structure, discipline and repeatable processes that ensure the core services are applied and used in a manner consistent with SWIM goals.

SWIM is developing and documenting Governance policies, processes and procedures that help define and allocate responsibilities among service providers, service consumers, the SWIM program, and other stakeholders (e.g., NAS approval authorities). As part of this activity, the SWIM service lifecycle is decomposed beyond the top-level treatment provided in this subsection and applicable policies and procedures are being defined for each lifecycle phase.

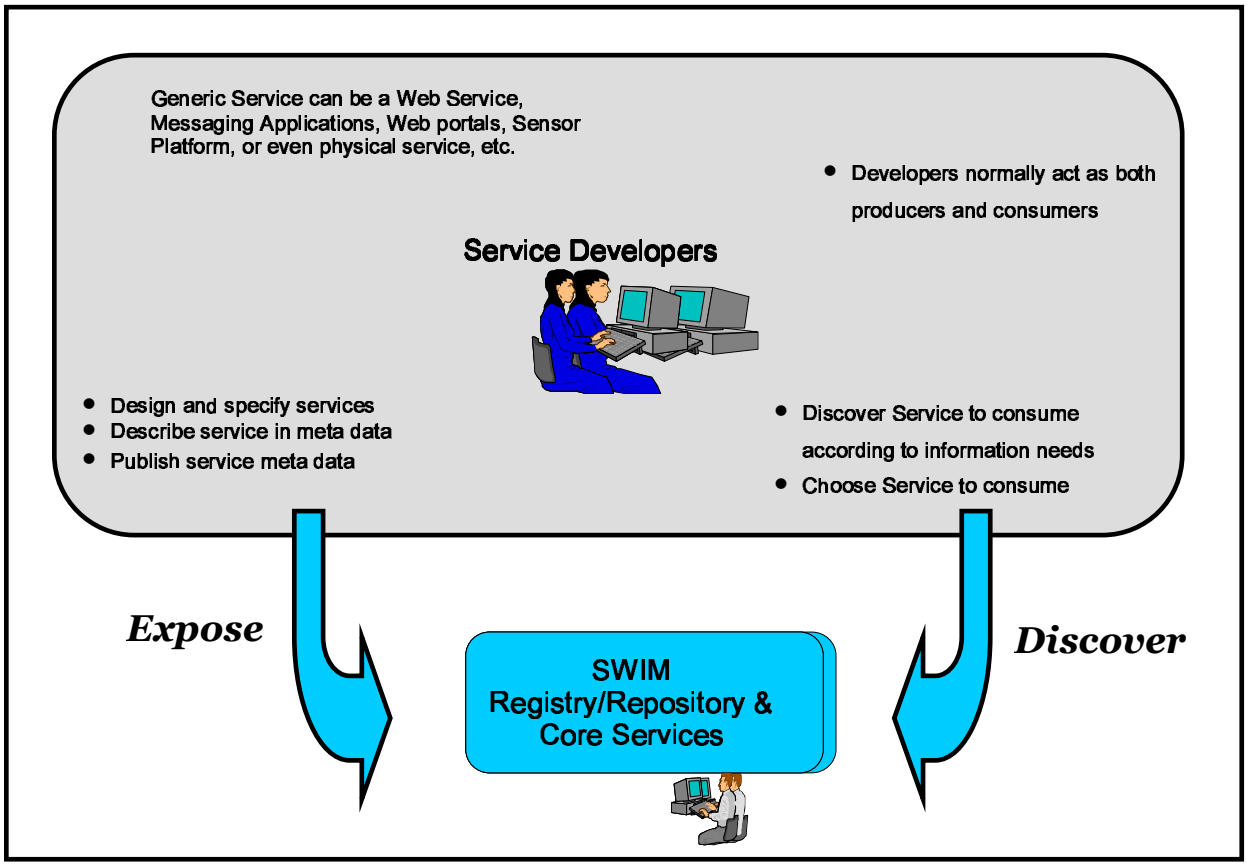
2.1.6.1 Design-Time (Development of Services)

The development of services begins when an operational need is identified and requirements are defined (prior to this, significant Governance-mandated portfolio management analyses occur). Requirements are elaborated and design decisions are

made, consistent with Governance policies, which shape the service delivery approach. In particular, services can be developed independently but often will leverage existing services to provide a composite capability. That is, the service being developed can itself be a consumer of other services.

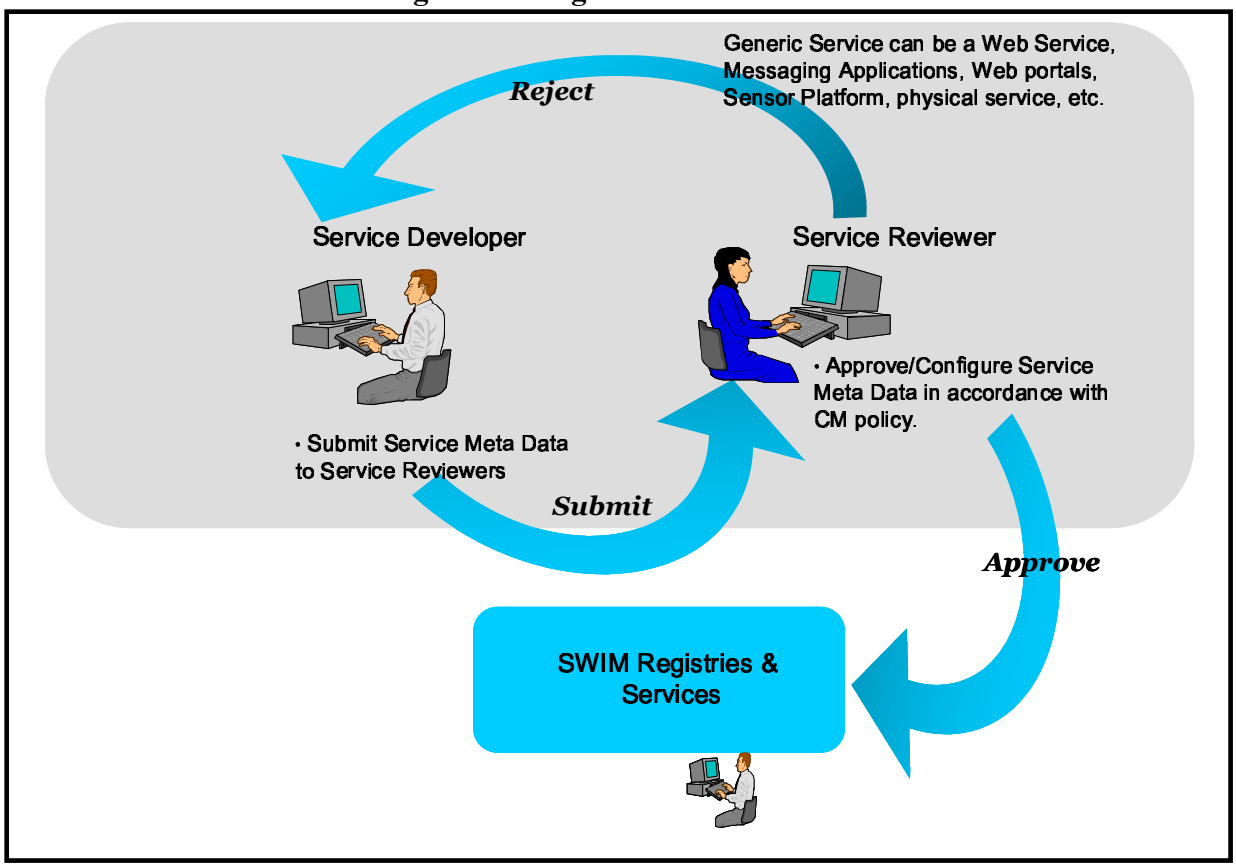
A service developer begins by using SWIM to discover available services. For example, a developer who wants to create a service that can forecast the arrival time of a flight at its destination airport may want to know what services are available that model flight trajectories. The developer will use SWIM interface management discovery capabilities to learn about the relevant services (e.g., through the service registry). Service descriptions are available that detail the input, output and performance characteristics. To promote reuse of services, SWIM registry policies ensure standardized service descriptions and classifications so that services are easily discoverable and their capabilities are well understood. When an appropriate reusable service is discovered, the developer can download a description of the service interface to enable it to be invoked by the new service. Security policies applicable to the service are used to ensure security-compliant service requirements are met. Similarly, service development is required to be performed consistent with applicable Governance policies and procedures. Figure 2-5 provides an illustration of service development.

Figure 2-5 Development of Services



In the design-time phase, the service description and service interface specification are reviewed. Figure 2-6 provides an illustration of service development, review and registration. Review and registration are elements of design-time phase. Non-compliant services are rejected and returned to the developers for correction. The Service reviewer is a notional role within a service development organization or SOA domain that evaluates services for compliance with applicable SWIM guidelines and policies. This activity is also performed independent of the service development organization as part of the Configuration Control Boards (CCB) process for the National Airspace System Change Proposal (NCP) containing the service or as part of the implementing program software QA process.

Figure 2-6 Registration of Services

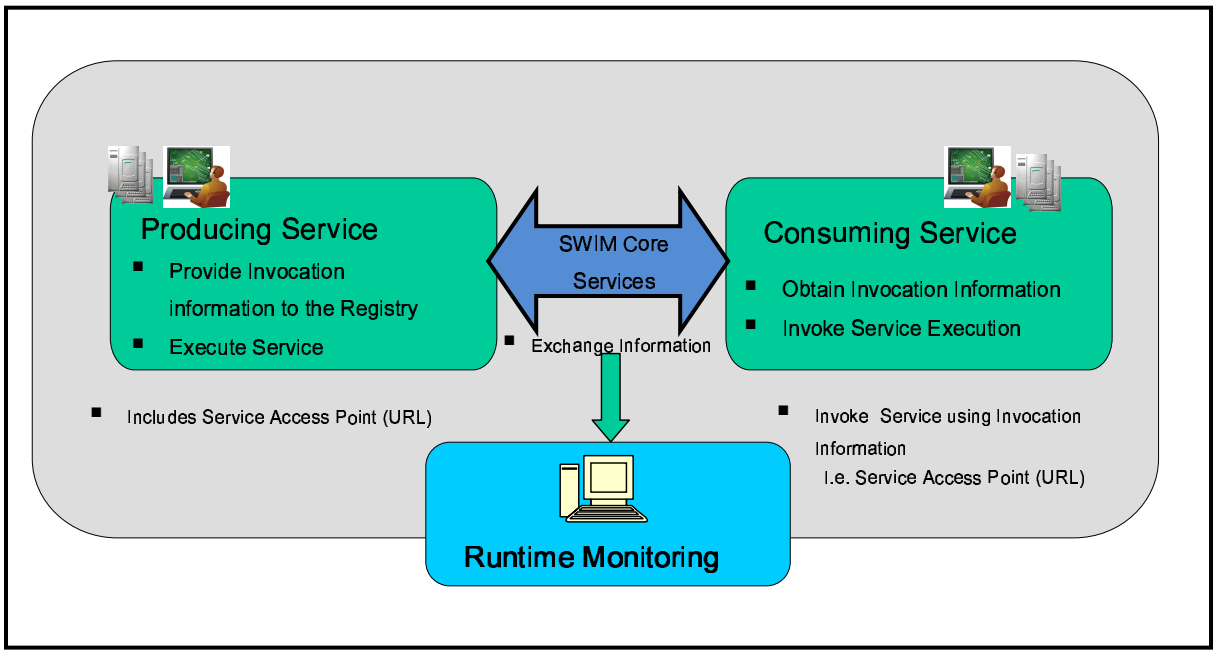


2.1.6.2 Run-Time (Deployment of Services)

Once a service is developed, approved, and registered it is placed at the appropriate resource (e.g., computers, portals or server platforms) for operational use. Consumers establish a relationship with the service provider to receive service on demand or repeatedly through a subscription. Service consumption is preceded by establishment of a formal Service Level Agreement (SLA) articulating expectations and assurances between service consumers and providers, consistent with Governance policy. This defines the beginning of the run-time phase of SWIM-enabled Services. The SWIM Enterprise Service Management and the Security Core Services monitor QoS metrics (e.g., the

latency, availability, and performance characteristics) and ensure security control mechanisms are in effect. Run-time Governance policies (e.g., regarding monitoring and failover mechanisms) promote robustness and reliability of SWIM operations. Figure 2-7 provides an illustration of runtime deployment of services.

Figure 2-7 Runtime Deployment of Services



Service exposure in the run-time phase occurs after the service has satisfied all testing and review requirements in its native development organization or SOA domain and it is placed into operations. The location of run-time service access point (e.g., URL for service endpoint location) for the operational service is registered to enable run-time service execution without the need for the service consumer to have that information. This enables agility as service location specifics change and ensures such details are transparent to the service consumer.

2.1.7 Governance

Successful SOA development and operations depend on well-defined policies and rules tailored to maintain order and consistency in the target environment. The SWIM program will enlist the support of the implementing programs in the development and execution of Segment 1 Governance plans that establish the required processes and capabilities. Governance includes management processes for all service lifecycle phases. The SWIM Segment 1 Governance primary focus is on design-time or the development phase. Segment 2 extends Governance to runtime operations and federates Governance consistent with the federation of functionality.

Governance establishes policies to assist in decision-making and accountability in developing and growing a SOA-based IT infrastructure. Governance is mandated by the distributed nature of services developed and implemented for SWIM-enabled systems in

various NAS organizational entities. Another compelling reason for SWIM Governance is the need to adhere to standards; consensus on, and adherence to, standards is achieved through a Governance mechanism. SWIM provides, communicates and helps enforce Governance Policies applicable to the SWIM program and its core services, the NAS Mission Services and the programs implementing Mission Services. Strategic SOA policies help support the overall direction and the future state of the SWIM SOA initiative. Service design-time policies apply to the context in which a service (or service version) is under development prior to its availability for consumption. Service Runtime and operational policies apply to the context in which a service (or service version) is available for consumption, regardless of its lifecycle stage. Runtime policies address non-functional requirements such as access, security, and performance. These policies are intended to ensure that desired organizational behaviors are achieved as needed to produce the desired enterprise SOA outcomes. For example, to ensure individual services conform to common design and technology standards for interoperability and reusability.

Some SWIM Governance policies mandate adherence to specific standards. For example, to enable service discovery, Strategic SOA policies include a mandate to adhere to FAA-STD-64, which specifies the content and structure of metadata describing registered services; FAA-STD-65 is mandated to describe as-built web service implementations in a Web Service Specification Document (WSSD); FAA-STD-63 is mandated to specify the construction and registration of FAA namespaces that are used to resolve ambiguity of Extensible Markup Language (XML) objects having different origins but the same names. Other standards related to technologies and products are also included as part of Governance to ensure interoperability.

Governance helps the disparate teams of architects across NAS organizational entities coordinate activities and work effectively together to create and maintain the elements of the SOA. It provides processes and policies specifying how and by whom services are released and maintained. SOA Governance influences activities to architect, design, develop, test and implement services. It also influences the methods employed to perform those activities, roles and responsibilities, and metrics to characterize success and adherence to policies.

2.1.7.1 Quality of Service

One of the most significant elements of Governance is QoS management. SOA's dynamic, flexible, and compositional nature requires that QoS management be integrated into service-oriented enterprise architectures. It must support a set of common QoS characteristics and provide comprehensive QoS services end to end, from application, to middleware, and to network and from source hosts to destination hosts across a network. SWIM Segment 1 begins the application of QoS management consistent with the defined importance of specific services to NAS operations. That is, QoS begins with a basic set of elements determined by the operational programs consistent with the requirements for critical, essential and routine services in accordance with NAS SR-1000, NAS System Requirements Specification. Segment 2 includes significantly more elements of QoS and SLAs are used to provide a record of agreements made on quality measures and expected and/or guaranteed levels of service quality.

2.1.7.2 Configuration Management

A critical element of Governance is Configuration Management (CM). CM covers all aspects of maintaining order across the system lifecycle, including establishing and modifying baselines (e.g., updating services and business processes). Consistent with SWIM's federated approach to SOA infrastructure and distributed Mission Services, a managed federated CM architecture is needed to manage and administer Mission Services distributed across SOA domains. CM of Core Services is federated in accordance with the technical capabilities and associated Governance policies and procedures. SWIM CM is based upon delegation of responsibilities among the appropriate CCB, SWIM Configuration Review Board (CRB), Communications CCB and a new body focused on enterprise-level issues associated with SOA, that is, a NAS Enterprise Services CCB (NESCCB). The NESCCB assists with portfolio management, in concert with the NAS EAB, to ensure a cohesive set of NAS services that meet NextGen objectives without duplication of effort. Each board has a specific set of related but complementary responsibilities that contribute to a cohesive SOA governance approach. Responsibilities of each board are defined in their respective CM Charters.

In Segment 1, the SWIM CRB will continue to exercise configuration control over all approved configuration items (CI) under the purview of the SWIM Program. NAS program legacy configuration items will continue under the CM of the SIPs based on their existing plans using existing program resources (augmented to ensure traceability between NAS program and SWIM program requirements). In Segment 2 the distribution of CM responsibilities will be realigned to provide appropriate support for the capabilities developed and operated in the SWIM SOA environment. The realignments will be responsive to characteristics of SWIM SOA, e.g., services that span multiple SOA domains.

In this environment, cross-organizational reuse of services creates dependencies among services for which CM approaches must be tailored. The focus of SWIM CM in Segment 2 is managing the service life-cycle (e.g., registry change control and service versioning to ensure continuity and to maintain operational status of services) coupled with support for building, releasing, deploying and maintaining shared services independently from each other. In particular, CM policies and mechanisms will ensure orderly transitions between versions of a service and the ability to support consumer needs in accordance with the Service Lifecycle Management Process. It will also address the need for an oversight body with CM authority over all services in order to effectively manage the SWIM portfolio and ensure alignment of NAS services with NextGen objectives without duplication of effort. SWIM Segment 2 CM will continue the migration away from the use of Interface Control Documents (ICDs) s to describe as-built interfaces. Instead, SWIM-supported interfaces will use modern means – such as the WSSD for web services.

2.1.7.3 Enterprise Information Management

Effective Enterprise Information Management (EIM) is a key determinant of successful SOA. EIM is also an aspect of Governance, establishing policies and executing procedures throughout the information lifecycle for structuring, describing and providing context for information assets (both structured and unstructured). EIM facilitates

standardized data sharing that improves operational efficiency and promotes cost-effective data exchange and interoperability. SWIM EIM ensures data is treated as an enterprise asset and helps ensure all sources of data are reconciled and consistent. SWIM EIM includes management of metadata to establish and maintain links between data and information assets.

SWIM EIM contributes to the goal of cost-effective information sharing by providing transparency related to data availability and discoverability, standardized data structures and semantics, data transformation requirements and by ensuring the integrity of data exchanges. SWIM EIM promotes these qualities in the data environment to help establish the requisite trust among stakeholders, enabling the transition from an ownership-oriented data environment to a stewardship-oriented data environment. EIM also enables improved performance analytics to support measurement of continuous improvement.

SWIM will provide an EIM methodology encompassing multiple interrelated elements such as shown in Figure 2-8.

Figure 2-8 High-Level EIM Methodology

EIM Planning	EIM Analysis	EIM Strategy	EIM Governance	EIM Implementation
✓ Vision ✓ Stakeholders ✓ Executive Buy-In ✓ Business Objectives ✓ Maturity Assessment ✓ Data Quality Audit ✓ Charter and Scope ✓ Success Metrics ✓ Roadmap	✓ Functional Areas ✓ Business Processes ✓ Information Types ✓ IT Architecture ✓ Current BI/DW Tools ✓ Current ECM Tools ✓ Data Inventory ✓ Information Flows ✓ Current Policies ✓ Search Use Cases ✓ Analysis Use Cases ✓ Decision Use Cases ✓ Gaps Analysis ✓ Redundancy Analysis	✓ Type Definitions ✓ Schema Definitions ✓ Interface Definitions ✓ Taxonomies ✓ Metadata Model ✓ Process Re-Design ✓ MDM Strategy ✓ Quality Strategy ✓ ECM Strategy ✓ BI Strategy ✓ SOA Strategy	✓ Data Stewards ✓ Security Policies ✓ Privacy Policies ✓ Retention Policies ✓ Quality Standards ✓ Process Management ✓ Data Management ✓ Content Management ✓ Change Management	✓ Tool Selection ✓ EIM Infrastructure ✓ Data Restructuring ✓ SOA Integration ✓ Data Services ✓ ETL Design ✓ Analytics Design ✓ Process Alignment ✓ Training ✓ Testing ✓ Deployment

2.1.8 Information Security

This subsection identifies the improvements that SWIM Segment 2 provides to address three of the five NAS security shortfalls identified in the report A NAS Security Architecture (MITRE, 2009). Enterprise information security capabilities enable the application of SOA principles. It is expected that the SWIM program may reallocate some of the requirements for these capabilities to other programs as appropriate. For example, FTI's NAS Enterprise Service Gateway (NESG) could implement certain security requirements.

1. A common enterprise boundary protection solution for the NAS is lacking. Currently, ad-hoc boundary protection solutions are created for each individual NAS system resulting in inconsistent solutions which may compromise the overall security of the NAS. In addition the ad-hoc approach leads to replication of efforts and complexity with the concomitant inadequate return on investment (waste of money) through the lifecycle of the multiple boundary protection solutions.

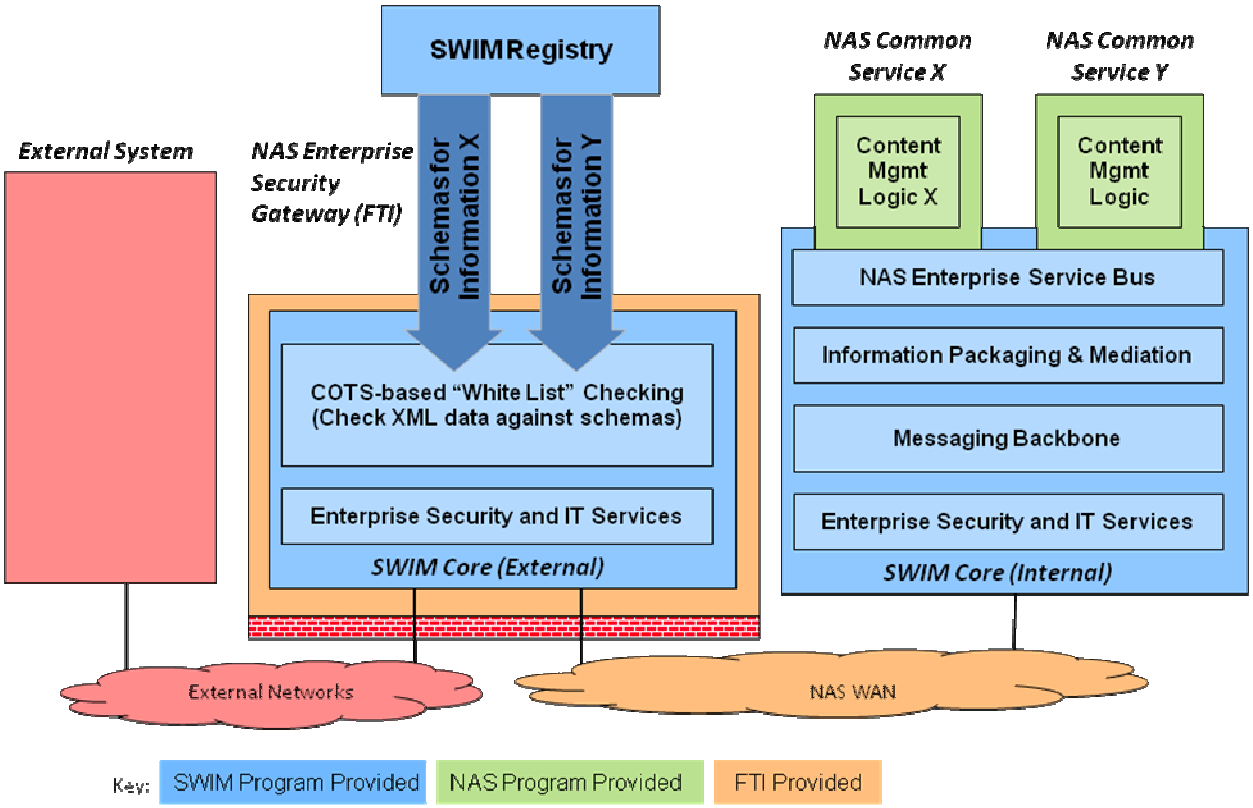
- SWIM will provide the NAS Enterprise Boundary Protection (EBP) capability. The EBP capability provides a set of security mechanisms that isolate NAS entities from non-NAS entities while still allowing information to be transferred into and out of the NAS as needed and authorized. As a NAS-wide enterprise service, the EBP capability is managed and operated by a single NAS organizational entity, and all data that flows into or out of the NAS will be subject to the security controls provided by the EBP capability.

2. A common enterprise identity verification and authorization capability for the NAS is lacking. These capabilities are essential for ensuring that only authorized individuals and systems are allowed to access (or update) NAS resources.
    - SWIM will provide the identification and authentication services that form the foundation of the NAS enterprise Identity and Key Management (I&KM) capability. These services allow users and machines to be identified, and also provides cryptographic key services that support provisioning and validation of digital credentials and keys as well as authentication (proof) of those identities. These services also make possible other security functions that rely on identities and keys, including confidentiality, integrity, and non-repudiation functions, wherever these functions are needed.
    - Another part of the I&KM capability provided by SWIM will be services that provide attribute information associated with system and user identities. These attributes can be used by other systems when those systems are performing Attribute Based Access Control (ABAC) to determine which users and systems are authorized to access different services and information.
    - SWIM will control access to SWIM core services and also will control access to NAS support services hosted on the SWIM core infrastructure.
    - The NAS enterprise I&KM capability will facilitate interoperability of security controls with NextGen partners.
    - As a NAS-wide enterprise service, the I&KM capability is operated and managed by a single organizational entity, and made available over the network to any point in the NAS where an interoperable identity and key-based security function is needed.
3. A common enterprise protection of NAS software management is lacking. Given the NAS continuously increasing reliance on commercially available software and customized software developed by contractors and subcontractors, the NAS requires a common approach to mitigate software vulnerabilities in the lifecycle phases after release, i.e., acquisition, storage, distribution, update, and disposal.
    - SWIM will provide the NAS Certified Software Management (CSM) capability. The capability consists of solutions to control access to software such that software executing on NAS equipment is guaranteed to be tested, and authorized for NAS use. The CSM capability will store and retrieve digitally signed or certified software updates, subject to enterprise policies including authentication, authorization, and auditing rules. As a

NAS-wide enterprise service, the CSM capability is operated and managed by a single organizational entity, and made available over the network to any point in the NAS where the ability to retrieve software updates from a secure central repository is needed. The result of CSM is that no system administrator as part of a software update operation would leave the secured NAS WAN to retrieve needed software. All automated, semi-automated and manual update procedure would point to the internal NAS repositories.

Figure 2-9 provides a conceptual overview of how SWIM supports these enterprise Information System Security (ISS) capabilities. It illustrates SWIM-provided capabilities (in blue) supporting mission-specific content management logic internal to the NAS, and also SWIM-provided capabilities supporting EBP within the NESG. I&KM and CSM services are part of "Enterprise Security and IT Services."

Figure 2-9 SWIM ISS Conceptual Overview



Other NAS programs provide ISS capabilities that complement those provided by SWIM. For example, programs providing Enterprise Services will include capabilities to audit use of these services and provide reports when anomalous events occur and prohibited activities are attempted. For example, NAS systems will detect and report attempts to use expired, revoked, suspended or otherwise improper or unauthorized identity credentials.

2.2 Maintenance

2.2.1 Hardware Maintenance

The operational SWIM infrastructure planned in Segment 1 will be developed and deployed by the implementing programs. The SWIM Program Office will purchase, and support for use by the implementing programs, hardware at the WJHTC for facilities to support system prototyping, development, integration and testing. The SWIM WJHTC facilities will be staffed and maintained by a combination of WJHTC and contractor staff, who will coordinate maintenance directly with the vendors from whom the hardware is purchased.

The SWIM implementing programs will be responsible for any hardware needed to host the SWIM software developed in Segment 1. Each program will provide hardware support in accordance with their existing plans.

SWIM Segment 2 consolidated SOA infrastructure will be developed and deployed by SWIM. SWIM will assume responsibility for all acquisition, management and maintenance activities for the hardware associated with consolidated SOA infrastructure (e.g., supporting SOA Core Services). Hardware associated with SOA capabilities federated outside the SWIM consolidated infrastructure will be the responsibility of the stakeholders hosting the federated capabilities. Each stakeholder will provide hardware support in accordance with their existing plans.

2.2.2 Software Maintenance

In SWIM Segment 1, the SWIM implementing program contractors, as directed by the implementing Program Offices, will develop the Segment 1 capabilities using SWIM-supplied software. SWIM implementing programs will integrate the SWIM Core Capabilities software and associated data into their services in accordance with their Software Development and Software Management Plans.

In SWIM segment 2, SWIM assumes responsibility for all acquisition, management and maintenance activities for the software associated with consolidated SOA infrastructure. Software associated with SOA capabilities federated outside the SWIM consolidated infrastructure will be the responsibility of the stakeholders hosting the federated capabilities. Each stakeholder will provide software support in accordance with their existing plans.

The maintenance concept for the SWIM-acquired commercial products will be Contractor Maintenance and Logistics Support (CMLS). SWIM implementing programs will use their current maintenance strategies to perform operational, maintenance, and support actions on deployed SWIM capabilities. SWIM will not require the development or introduction of new FAA job categories or skill classifications over and above what is currently in the NAS, for the purposes of operation and maintenance of SWIM

2.2.3 Quantities and Locations

2.2.3.1 Segment 1

Table 2-1 provides a summary of SWIM Segment 1 systems and locations, organized by the implementing program. The number of sites includes the FAA William J. Hughes Technical Center (WJHTC) and the FAA Air Traffic Control System Command Center (ATCSCC), as appropriate. It does not include the development contractor sites to which development systems may be deployed.

Table 2-1. SWIM Segment 1 Sites and Location

COI	Implementing Program	# Sites	Location	Comments
AIM	AIM	2	FAA Headquarters and ATCSCC	Hardware and software
AIM	ERAM AIM	22	ARTCCs, WJHTC, FAAAC	Software, only
F&FM	TFM	2	WJHTC, VNTSC	Hardware and software
	ERAM	22	ARTCCs, WJHTC, FAAAC	Hardware and software
	Terminal	38	Major TRACONs and ATCTs	Hardware and software
WX	ITWS	1	VNTSC	Hardware and software
	CIWS	1	WJHTC	Software, only
	WMSCR	3	Atlanta & Salt Lake City NNCCs, WJHTC	Hardware and software
	ERAM WMSCR	22	ARTCCs, WJHTC, FAAAC	Software, only
Core Capabilities	N/A	2	WJHTC, ATCSCC	Hardware and software

2.2.3.2 Segment 2

2.2.3.3

The following provides a summary of SWIM Segment 2 SOA infrastructure hardware and software locations. Systems and locations for hardware and software provided by other systems (e.g., Mission Services) are not shown. Those determinations will be made by the respective programs.

There are numerous possible physical architecture options. The following preliminary architecture is based on the need to enable ready access to telecommunications infrastructure and communications gateways while maintaining geographic diversity and CONUS coverage. The existing ARTCCs and gateway locations provide a number of

ready site location options that satisfy this need. The subset of these sites identified below is expected to be able to provide a sufficient solution. Nine sites are included.

Six ARTCC sites include: Seattle (ZSE), Chicago (ZAU), Boston (ZBW), Leesburg (ZDC), Dallas Fort Worth (ZFW), Los Angeles (ZLA).

Three gateway sites: Atlanta NNCC (collocated with Atlanta ARTCC), Salt Lake NNCC (collocated with Salt Lake ARTCC), WJHTC in Atlantic City.

All sites include SWIM-provided hardware (e.g., servers and communications equipment) and software (e.g., message brokers, ESBs). ARTCC sites are expected to include the following hardware: core application, web and database servers; ESBs and message brokers; XML gateway servers; shared storage; and communications equipment (e.g., LAN, switches and routers). Gateway sites are expected to include the following hardware: Key and Certificate servers; directory, web proxy, XML gateway and DNS servers; ESM and runtime policy management servers; shared storage; and communications equipment (e.g., LAN, switches and routers).

Software components allocated to these sites include products providing the following capabilities: DNS; ESB, message brokers, adapters and frameworks; database; registry/repository; security-related software such as XML Gateway, key and certificate server, directory server and proxies. Many of these software components are available as COTS products.

2.2.4 Schedule Constraints

2.2.4.1 Segment 1

The overall program strategy is to conduct a phased development approach. Each of the implementing programs has developed their own schedule for their Segment 1 SWIM-enabled capability, and the SWIM program is working to ensure that the Core Capabilities will be available in time to support the implementing programs' schedules.

Starting in late FY08, the SWIM program will provide each implementing program with "GFE from SWIM" software and data packages that provide the SWIM-required protocols, messaging, and interface management capabilities. Identifying the software packages by late FY08 is a schedule constraint so that implementing programs can incorporate the SWIM capability in their planned release schedules.

The Initial Flight Data Services, part of the ERAM Flight Data Services capability, will be the first to use the SWIM Core Capabilities. During ERAM Release 2, Initial Flight Data Services will incorporate the "GFE from SWIM" software and data packages into their release design, and will complete code and test to support ERAM's Release 2 deployment.

Shortly thereafter, a standalone AIM capability and CIWS will become SWIM-enabled. At a later date, TFMS, terminal services, ITWS, WMSCR, and AIM with ERAM will become SWIM-enabled. These capabilities are not interdependent, but do rely on the availability of Core Capabilities. The final capability planned for Segment 1 will be developed by ERAM – SWIM publication of Runway Visual range (RVR) data. This

capability depends on the deployment of the new Terminal Data Distribution System (TDDS), which is completed in FY14.

2.2.4.2 Segment 2

The phased development approach continues into Segment 2. Each program implementing service consumer and provider capabilities (e.g., Mission Services) develops their own schedule consistent with the NASEAF Roadmap. The SWIM program is working to ensure that the SOA infrastructure will be available in time to support these programs' schedules.

The Development of the SWIM SOA infrastructure (Core Services) is scheduled to begin in FY2Q12, immediately after award of the associated acquisition contract. The development activity will include two sequential Phases with the Phase 1 ending in FY1Q14 and Phase 2 ending in FY4Q15.

Implementation of program capabilities (e.g., Mission Services) is expected to follow a waterfall pattern. That is, each major capabilities package is implemented sequentially. Capabilities will be implemented in phases consistent with the Core Services Phases. Core Services Phase 1 will be in place prior to, and provide support to, two capability packages associated with the NNEW, AIM and ASIAS programs. The first Phase 1 package begins development in FY2Q13 and ends in FY1Q14. The second Phase 1 package begins development in FY2Q14 and ends in FY3Q14.

Core Services Phase 2 will be in place prior to, and provide support to, two capability packages associated with the En Route, AIM-M2, RMLS, Terminal, TFM and NWP programs. The first Phase 2 package begins development in FY1Q15 and ends in FY1Q16. The second Phase 2 package begins development in FY2Q16 and ends in FY4Q16.

3.0 Technical Performance

Section 3 includes legacy requirements from Segment 1 and new Segment 2 requirements. All requirements are organized consistent with the SV-4b diagram presented in Figure 1-1. Segment 1 requirements language is unchanged from the original baselined and approved form, but the requirements are in differently numbered subsections compared to the Segment 1 FPR. Therefore, the Segment 1 requirements numbers have changed to conform to the current subsection numbering. To help delineate Segment 1 and Segment 2 requirements, Segment 2 requirements include a suffix: "(Segment 2)." All legacy Segment 1 requirements also apply to Segment 2 unless appended with the suffix "(Segment 1 Only)."

The following subsections define SWIM capabilities associated with the elements of the NASEAF. The definition of each NASEAF element (layer) is provided in Table 1-1 and is intended to be used as context for the requirements in each subsection. These definitions are provided for context, not to levy SWIM requirements.

3.1 Operational and Functional Requirements

SWIM provides capabilities to users that have been granted permission to access these capabilities. Numerous requirements in this document include qualifiers that emphasize the need for restrictions on user access. The terms “authorized user” and “registered user” are both used to indicate the ability to classify users and grant permissions based on class or other user attributes. The following provides an example of how this terminology is used:
SWIM shall enable sharing of information among registered users.

3.1.1 Interaction Services

3.1.1.1 On-Demand NAS Portal

3.1.1.1.1 SWIM shall provide a portal to support design-time activities of non-NAS consumers (consumers external to the NAS). (Segment 2)

3.1.1.1.2 SWIM shall provide a portal to support run-time activities of non-NAS consumers (consumers external to the NAS). (Segment 2)

3.1.1.2 Administrative Portal

3.1.1.2.1 SWIM shall provide a portal to support design-time activities for NAS consumers (consumers internal to the NAS). (Segment 2)

3.1.1.2.2 SWIM shall provide a portal to support run-time activities for NAS consumers (consumers internal to the NAS). (Segment 2)

3.1.1.3 Browser - Reserved

3.1.1.4 Client - Reserved

3.1.1.5 Weather Notification - Reserved

3.1.1.6 Flow Constraint Notification - Reserved

3.1.1.7 Airport Status and Mission Critical Notification - Reserved

3.1.2 Mission Services - Reserved

3.1.3 Support Services

3.1.3.1 Data Access

3.1.3.1.1 Content Discovery

3.1.3.1.1.1 SWIM shall provide run-time enterprise-level content discovery. (Segment 2)

3.1.3.1.1.2 SWIM shall support information queries between systems implemented by other programs. (Segment 2)

3.1.3.1.1.3 SWIM shall aggregate information retrieved from systems implemented by other programs in accordance with predefined business rules. (Segment 2)

3.1.3.1.1.4 SWIM shall support EIM in accordance with predefined business rules (including single authoritative information source definitions) associated with Enterprise Services. (Segment 2)

3.1.3.1.2 Data Acquisition

3.1.3.1.2.1 SWIM shall support queries or mechanisms for passive receipt of persistent data required by the Mission Services.

3.1.3.1.3 Service Adaptation

3.1.3.1.3.1 SWIM shall provide the adaptation or transformation required to enable legacy services or applications to use SOA Core Services to exchange information with other services. (Note: Service Adaptation allows legacy applications to achieve service orientation without change to the legacy application logic.)

3.1.3.2 Data Flow Management

3.1.3.2.1 Data Composition

3.1.3.2.1.1 SWIM shall support manipulation of data to match the composition of Mission Services to support performance and scalability.

3.1.3.2.2 Data Flow Mechanisms

3.1.3.2.2.1 SWIM shall support movement of information as needed to satisfy data flow requirements of the Mission Services. (Examples might include processing and enriching data in bulk or unique domain driven batch processing activities.)

3.1.4 SOA Core Services

3.1.4.1 Interface Management

3.1.4.1.1 SWIM Publication Services

3.1.4.1.1.1 SWIM shall build a Service Registry for deploying information about SWIM services.
3.1.4.1.1.2 SWIM shall add information to the Service Registry.
3.1.4.1.1.3 SWIM shall modify information in the Service Registry.
3.1.4.1.1.4 SWIM shall delete information from the Service Registry.
3.1.4.1.1.5 SWIM shall provide configuration management for information in the Service Registry.
3.1.4.1.1.6 SWIM shall maintain the changes of operational status for services in the Service Registry.

3.1.4.1.2 Service Discovery

Service Discovery provides the capability for service consumers to be able to easily find information about services including the service access point.

3.1.4.1.2.1 SWIM shall search the SWIM Service Registry for service definitions and service interface information for registered users.

3.1.4.1.2.2 SWIM shall retrieve from the SWIM Service Registry for service definitions and service interface information for registered users.
3.1.4.1.2.3 SWIM shall manage access to information in the service registry. (Segment 2)
3.1.4.1.2.4 SWIM shall provide an information repository to store service metadata and service descriptions. (Segment 2)
3.1.4.1.2.5 SWIM shall SWIM shall manage access to information in the SWIM repository. (Segment 2)
3.1.4.1.2.6 SWIM shall provide configuration management of information in the SWIM repository. (Segment 2)

3.1.4.1.3 Service Registration

Service Registration provides a means for the service providers to register service descriptions, including service SLA and QoS characteristics, and metadata for Service Interfaces.

3.1.4.1.3.1 SWIM shall monitor the Service Registry with changes including new services commissioned, replaced services, and decommissioned services.
3.1.4.1.3.2 SWIM shall allow registered users to subscribe to notifications when registry information changes in accordance with new services commissioned, replaced services, and decommissioned services
3.1.4.1.3.3 SWIM registered users shall define the terms of their registry subscription.
3.1.4.1.3.4 SWIM registered users shall modify the terms of their registry subscription.
3.1.4.1.3.5 SWIM shall provide the capability for service providers to expose Service Registry information to authorized users. (Segment 2)

3.1.4.2 Messaging Services

3.1.4.2.1 General Messaging

3.1.4.2.1.1 Reliable Messaging

Reliable Messaging provides support for guarantees of message delivery.

3.1.4.2.1.1.1 SWIM shall provide messaging that delivers messages once and only once. (Segment 2)

3.1.4.2.1.1.2 SWIM shall provide messaging that guarantees delivery in accordance with QoS criteria. (Segment 2)

3.1.4.2.1.1.3 SWIM shall provide messaging that can deliver messages in a prescribed order. (Segment 2)

3.1.4.2.1.1.4 When message delivery failure occurs, SWIM shall notify both the sender and receiver in accordance with QoS criteria. (Segment 2)

3.1.4.2.1.2 Message Transport

Message Transport provides multiple application-level transports to any endpoint. SWIM supports several transport protocols. Transmission Control Protocol (TCP) is one of the

core protocols of the Internet Protocol Suite. TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. The Hypertext Transfer Protocol (HTTP) is a request/response standard protocol for distributed, collaborative, hypermedia information systems. Transport Layer Security (TLS) is a cryptographic protocol that provides security for communications over networks such as the Internet. Hypertext Transfer Protocol Secure (HTTPS) is a combination of the HTTP and the TLS protocol to provide encryption and secure identification of the server. SOAP, originally defined as *Simple Object Access Protocol*, is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. Apache ActiveMQ is an open source message broker which fully implements the Java Message Service (JMS).

3.1.4.2.1.2.1 SWIM shall support services using the SOAP-over-HTTP/HTTPS message transport protocol. (Segment 2)

3.1.4.2.1.2.2 SWIM shall support services using the XML-over-HTTP/HTTPS message transport protocol, inclusive of the Representative State Transfer (REST) interface pattern. (Segment 2)

3.1.4.2.1.2.3 SWIM shall support services using the SOAP-over-ActiveMQ-over-HTTP/HTTPS message transport protocol. (Segment 2)

3.1.4.2.1.2.4 SWIM shall support services using the ActiveMQ over TCP / TCP + TLS message transport protocol. (Segment 2)

3.1.4.2.1.3 Message Integrity and Confidentiality

Message integrity mechanisms ensure that message contents are received exactly as sent, i.e., unaltered. Message confidentiality mechanisms ensure that only intended parties in a message exchange can view messages.

3.1.4.2.1.3.1 SWIM shall protect message content from unauthorized manipulation, alteration or compromise. (Segment 2)

3.1.4.2.1.3.2 SWIM shall protect messages from disclosure to unauthorized persons. (Segment 2)

3.1.4.2.2 Message Routing

Message Routing provides support for messages routing between service providers and service consumers.

3.1.4.2.2.1 SWIM shall record the locations of Service Providers and Service Consumers at design-time.

3.1.4.2.2.2 SWIM shall provide run-time message routing between Service Consumers and Service Providers using their current recorded location.

3.1.4.2.2.3 SWIM shall provide message routing based on message content. (Segment 2)

3.1.4.2.2.4 SWIM shall provide message routing based on environmental conditions including system state and loading. (Segment 2)

3.1.4.2.2.5 SWIM shall provide message routing based on a fixed, predefined sequence (itinerary) of recipients. (Segment 2)
3.1.4.2.2.6 SWIM shall provide message routing that enables complex workflow management in accordance with predefined business rules. (Segment 2)
3.1.4.2.2.7 SWIM shall provide message routing that enables extended, stateful dialogs among services. (Segment 2)

3.1.4.2.3 SWIM Run-Time Business Service Subscriber Status

3.1.4.2.3.1 SWIM shall monitor Business Service Subscriber Status.
3.1.4.2.3.2 SWIM shall alter message routing consistent with Business Service Subscriber Status.

3.1.4.2.4 Design-Time Business Service Message Management

3.1.4.2.4.1 SWIM shall publish and route messages and alerts to subscribing Service Consumers.
3.1.4.2.4.2 SWIM shall ensure messages and alerts are delivered as specified in accordance with service level agreements.

3.1.4.2.5 Publish-Subscribe

Publish-Subscribe provides support for publish-subscribe message exchange pattern.

3.1.4.2.5.1 SWIM shall provide services that support a publish-subscribe message exchange pattern. (Segment 2)

3.1.4.2.6 Request-Response

Request-Response provides support for the request-response message exchange pattern.

3.1.4.2.6.1 SWIM shall provide services that support a Request-Response message exchange pattern. (Segment 2)

3.1.4.2.7 Mediation

Mediation provides the capability for various types of mediation such as data format transformation, between message senders and receivers.

3.1.4.2.7.1 SWIM shall provide mediation between message transport protocols. (Segment 2)
3.1.4.2.7.2 SWIM shall provide mediation between data representations. (Segment 2)
3.1.4.2.7.3 SWIM shall provide mediation between data types. (Segment 2)
3.1.4.2.7.4 SWIM shall provide mediation between data structures. (Segment 2)

3.1.4.3 SWIM Security Services

SWIM Security Services focuses on requirements provided by SWIM as services to the rest of the NAS.

3.1.4.3.1 General SWIM Security Services Requirements

3.1.4.3.1.1 SWIM shall provide security services capabilities in accordance with FAA Order 1370.82A, Information Systems Security Policy. (Segment 2)

3.1.4.3.1.2 SWIM shall provide security services capabilities in accordance with FAA Order 1370.104, Digital Signature Policy. (Segment 2)

3.1.4.3.1.3 SWIM shall provide security services capabilities in accordance with FAA Order 1370.95, Wide Area Network Connectivity Security. (Segment 2)

3.1.4.3.1.4 SWIM shall provide security services capabilities in accordance with the NAS ISS Roadmap contained in the NAS Enterprise Architecture. (Segment 2)

3.1.4.3.2 SWIM Run-Time Access Management

3.1.4.3.2.1 SWIM shall implement service security policies which require a SWIM member to register member identification and access privileges.

3.1.4.3.2.2 SWIM shall grant access to all SWIM services, transactions, and information in accordance with member identification and access privileges

3.1.4.3.3 SWIM Security Administration

3.1.4.3.3.1 SWIM shall publish SWIM service security policies for design-time implementation and run-time monitoring.

3.1.4.3.3.2 SWIM shall enable design-time modification of SWIM service security policies.

3.1.4.3.3.3 SWIM shall propagate SWIM service security policies at design-time.

3.1.4.3.3.4 SWIM shall detect service security events at design-time.

3.1.4.3.3.5 SWIM shall record service security events and associated data at design-time.

3.1.4.3.3.6 SWIM shall analyze and report service security events and associated data at design-time.

3.1.4.3.4 SWIM Run-Time Security Support

3.1.4.3.4.1 SWIM shall monitor and record run-time transactions in accordance with SWIM service security policy.

3.1.4.3.4.2 SWIM shall formulate and issue run-time service security alerts.

3.1.4.3.5 Security Policy Enforcement and Access Management

Security Policy Enforcement provides mechanisms to enforce specific rules set by the NAS SOA Governance body that derive from formal security policies. Access Management provides management of access to data resources that are based on the requesting entity's identity, organizational role, or other considerations such as transaction state or application. For example, Access Management includes mechanisms to enforce message integrity and confidentiality rules.

3.1.4.3.5.1 SWIM shall provide a standardized service interface layer for security policy enforcement. (Segment 2)

3.1.4.3.5.2 SWIM shall provide a standardized service interface layer for data access management. (Segment 2)

3.1.4.3.6 Service Security Monitoring

Service Security Monitoring provides monitoring of NAS services for any systems events that may indicate security breach or fraudulent use of NAS system resources.

3.1.4.3.6.1 SWIM shall include instrumentation of networks and systems to gather data relevant to security monitoring. (Segment 2)

3.1.4.3.6.2 SWIM shall provide security monitoring data collected from SWIM networks and systems (including network intrusion detection sensor data, system logs, etc.) to a designated external intrusion detection and response facility (e.g., the Cyber Security Management Center (CSMC). (Segment 2)

3.1.4.4 SWIM Enterprise Services Management

3.1.4.4.1 SWIM Run-Time QoS Management

3.1.4.4.1.1 SWIM shall define SWIM QoS criteria and metrics for run-time monitoring

3.1.4.4.1.2 SWIM shall modify SWIM QoS criteria and metrics for run-time monitoring.

3.1.4.4.1.3 SWIM shall propagate SWIM QoS criteria and metrics.

3.1.4.4.1.4 SWIM shall detect QoS events.

3.1.4.4.1.5 SWIM shall record QoS events and associated data.

3.1.4.4.1.6 SWIM shall analyze and report QoS events and associated data.

3.1.4.4.2 SWIM Run-Time Support Infrastructure Maintenance

3.1.4.4.2.1 SWIM shall detect SWIM Support Infrastructure failure events including overloads and faults.

3.1.4.4.2.2 SWIM shall record SWIM Support Infrastructure failure events and associated data.

3.1.4.4.2.3 SWIM shall analyze and report SWIM Support Infrastructure failure events and associated data.

3.1.4.4.2.4 SWIM shall automatically recover from SWIM Support Infrastructure failure events.

3.1.4.4.2.5 SWIM shall automatically isolate failed SWIM Support Infrastructure assets.

3.1.4.4.2.6 SWIM shall maintain an inventory of all active and previously active SWIM Support Infrastructure assets.

3.1.4.4.3 Policy Enforcement and Metrics Collection

Policy Enforcement and Metrics Collection enforces policies set by the governance process including SLA compliance and message QoS compliance.

3.1.4.4.3.1 SWIM shall enforce policies set by the SWIM governance process. (Segment 2)

3.1.4.4.3.2 SWIM shall collect and maintain metrics on policy compliance and enforcement actions. (Segment 2)

3.1.4.4.4 SLA Compliance and Metrics Collection

SLA Compliance and Metrics Collection monitors services to determine if factors specified in Service Level Agreements (SLAs) are out of the permitted range, including but not limited to resource utilization, fault behaviors, and performance metrics.

3.1.4.4.4.1 SWIM shall monitor SLA compliance. (Segment 2)
3.1.4.4.4.2 SWIM shall record metrics on SLA compliance. (Segment 2)
3.1.4.4.4.3 (Segment 2)
3.1.4.4.4.4 SWIM shall record all deviations from SLA compliance. (Segment 2)
3.1.4.4.4.5 SWIM shall provide reports on SLA compliance metrics to authorized users. (Segment 2)

3.1.4.4.5 Performance Monitoring and Reporting

Performance Monitoring and Reporting monitors services to determine level of performance including but not limited to throughput and response time. It also generates threshold based alerts and reports performance based metrics.

3.1.4.4.5.1 SWIM shall monitor QoS metrics including service performance. (Segment 2)
3.1.4.4.5.2 SWIM shall record QoS metrics. (Segment 2)
3.1.4.4.5.3 SWIM shall provide the capability to set QoS metric threshold values. (Segment 2)
3.1.4.4.5.4 SWIM shall generate an alert when a QoS metric threshold value is exceeded. (Segment 2)
3.1.4.4.5.5 SWIM shall provide QoS metrics reports to authorized users. (Segment 2)

3.1.4.4.6 Fault Monitoring and Reporting

Fault Monitoring and Reporting monitors services to determine if a service has a fault and reports the fault.

3.1.4.4.6.1 SWIM shall monitor service faults. (Segment 2)
3.1.4.4.6.2 SWIM shall record service faults. (Segment 2)
3.1.4.4.6.3 SWIM shall report service faults. (Segment 2)

3.1.4.5 Collaboration Services - Reserved

3.1.5 Technical Infrastructure Services

3.1.5.1 Boundary Protection

Boundary Protection provides appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) monitors and controls communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications. (Note: It is expected that SWIM will utilize FTI services such as the NESG services to support implementation of the requirements in this section.)

3.1.5.1.1 Common Provisions

3.1.5.1.1.1 SWIM shall provide an EBP capability for the NAS that reduces the risk that information exchanges between NAS entities and external (non-NAS)

entities will compromise the confidentiality, integrity, or availability of the NAS. (Segment 2)

3.1.5.1.1.2 SWIM shall provide an EBP facility (or set of facilities), under common management and operational control, to mediate information transfers between internal NAS entities and external entities. (Segment 2)

3.1.5.1.1.3 SWIM shall provide connectivity to the SWIM EBP facility via a common NAS-wide IP network using a common IP address structure. (Segment 2)

3.1.5.1.1.4 SWIM shall provide an EBP capability that logically consolidates all NAS cyber connections that transfer data to external entities (non-NAS entities, or NAS entities that cannot be guaranteed to operate to a sufficient level of cyber security). (Segment 2)

3.1.5.1.1.5 SWIM shall provide boundary throughput, fault and other performance data to authorized users. (Segment 2)

3.1.5.1.1.6 SWIM shall provide an EBP capability that ensures that each information transfer between NAS internal and external entities is temporarily stored, checked and processed (i.e., "staged") in accordance with other SWIM EBP requirements, before being forwarded to its destination. (Segment 2)

3.1.5.1.1.7 SWIM shall allow each NAS internal entity to control the rate and frequency of data transfers between that entity and SWIM EBP staging devices. (Segment 2)

3.1.5.1.1.8 SWIM shall provide an EBP capability that prevents any external entity from directly connecting to any NAS internal entity. (Segment 2)

3.1.5.1.2 Aviation Partner Access Provisions

The term "Aviation Partner" is used herein to identify a designated external entity that the FAA has explicitly determined should be allowed to access specific FAA resources.

3.1.5.1.2.1 SWIM shall provide IP network connectivity between the EBP capabilities and aviation partners to allow information exchange with the NAS. (Segment 2)

3.1.5.1.2.2 SWIM shall support aviation partner access to the EBP capabilities via the TCP/IP protocol suite. (Segment 2)

3.1.5.1.2.3 SWIM shall provide aviation partner access over networks or connections that are segregated (as needed based on program requirements) from the public Internet. (Segment 2)

3.1.5.1.2.4 SWIM shall ensure that aviation partners and NAS devices are required to provide strong proof of their identity (mutual authentication). (Segment 2)

3.1.5.1.2.5 SWIM shall provide the option for aviation partner access through user (human) authentication controls for data transfer to and from the NAS. (Segment 2)

3.1.5.1.2.6 SWIM shall provide integrity assurances for all information transfers for aviation partner access. (Segment 2)

3.1.5.1.2.7 SWIM shall provide the option for aviation partner access with data confidentiality controls for data transfer to and from the NAS. (Segment 2)

3.1.5.1.2.8 SWIM shall provide aviation partner authentication, integrity and confidentiality controls based on the solutions specified within the I&KM capability. (Segment 2)

3.1.5.1.2.9 SWIM shall provide aviation partner access that supports the placement of data on and retrieval of data from staging devices within the EBP facility. (Segment 2)

3.1.5.1.3 Public Access Provisions

3.1.5.1.3.1 SWIM shall provide an EBP capability to support public access of NAS information. (Segment 2)

3.1.5.1.3.2 SWIM shall provide an EBP capability for public access via the public Internet. (Segment 2)

3.1.5.1.3.3 SWIM shall provide public access to the EBP capabilities only to a pre-approved set of NAS staging devices contained within the controlled EBP environment. (Segment 2)

3.1.5.1.3.4 SWIM shall provide public EBP access limited to the ability to retrieve data from servers that are resident within the EBP. (Segment 2)

3.1.5.1.3.5 SWIM shall isolate the NAS staging devices that have Internet Access from other NAS and EBP elements. (Segment 2)

3.1.5.1.3.6 SWIM shall provide public EBP access with authentication, integrity and confidentiality controls as options for transfer of data. (Segment 2)

3.1.5.1.4 Non-IP Data Transfer Provisions

3.1.5.1.4.1 SWIM shall provide EBP access capable of supporting the use of non-IP based network transfers, including X25 packet layer, HDLC its variants and ATN for access to the NAS, once the need is determined by a NAS program. (Segment 2)

3.1.5.1.4.2 SWIM shall provide an EBP capability that consolidates all external non-IP access using a common facility (or set of facilities). (Segment 2)

3.1.5.1.4.3 SWIM shall provide an EBP capability that uses NAS program-supplied functionality to convert from specific legacy non-IP information flows to IP-based information flows. (Segment 2)

3.1.5.1.4.4 SWIM shall provide an EBP capability that limits access to the NAS interior to an IP-based information flow.

3.1.5.1.4.5 SWIM shall provide an EBP capability for non-IP data transfers that support the placement of data on and retrieval of data from staging devices within the EBP. (Segment 2)

3.1.5.1.5 Remote Administrative Access Provisions

3.1.5.1.5.1 SWIM shall provide an EBP capability for remote administrative access for system administrators, NAS technicians and other approved individuals to access internal NAS elements from outside the NAS. (Segment 2)

3.1.5.1.5.2 SWIM shall provide an EBP capability to restrict remote administrative access to a pre-approved list of specific NAS system elements. (Segment 2)

3.1.5.1.5.3 SWIM shall provide an EBP capability to restrict remote administrative access to pre-approved individuals. (Segment 2)

3.1.5.1.5.4 SWIM shall enforce data integrity, authentication and confidentiality controls for all EBP data transfers through administrative access. (Segment 2)
3.1.5.1.5.5 SWIM shall restrict the EBP remote administrative access capability to users providing strong proof (authentication) of their identity. (Segment 2)
3.1.5.1.5.6 SWIM shall provide remote administrative access via the Internet and/or the public switched telephone network. (Segment 2)
3.1.5.1.5.7 SWIM shall provide wireless connectivity in accordance with FAA Order 1370.94. (Segment 2)
3.1.5.1.5.8 SWIM shall provide remote administrative access over private networks or virtual private networks (VPNs). (Segment 2)
3.1.5.1.5.9 SWIM shall securely provide administrative access server addresses within the EBP to authorized administrative personnel and systems. (Segment 2)
3.1.5.1.5.10 SWIM shall prohibit administrative server addresses within the EBP from being advertized by any means. (Segment 2)
3.1.5.1.5.11 SWIM shall provide a proxy server within the EBP facility to relay administrative data to and from the NAS interior. (Note this is required as all connections must terminate within the EBP).
3.1.5.1.5.12 SWIM shall ensure the confidential connection ends on the proxy server and is re-established to access the interior NAS. (Segment 2)
3.1.5.1.5.13 SWIM shall provide anti-virus checks for all data transfers.
3.1.5.1.5.14 SWIM shall prevent data failing anti-virus checks from being forwarded. (Segment 2)
3.1.5.1.5.15 SWIM shall provide an alert to the administrator or field technician transferring data which has failed an anti-virus check. (Segment 2)

3.1.5.1.6 Guard Gateway Provisions ("Data White-Listing")

3.1.5.1.6.1 SWIM shall provide EBP guard gateways that are transparent to the data flow (i.e. neither sender nor receiver need to change their operation due to the flow passing through the guard gateways). (Segment 2)
3.1.5.1.6.2 SWIM shall ensure EBP guard gateways examine all application data entering or leaving the NAS with the possible exception of administrative-access transfers. (Segment 2)
3.1.5.1.6.3 SWIM shall ensure that the use of EBP guard gateways for administrative access is pre-determined by the functions being performed. (Segment 2)
3.1.5.1.6.4 SWIM shall ensure that EBP guard gateways utilize previously approved format and protocol definitions (e.g. schemas) that define the expected type, length, and range of data fields composing an application message. (Segment 2)
3.1.5.1.6.5 SWIM shall provide an EBP guard gateway capability to block the passage of application messages containing data that does not conform to pre-defined formats or protocols. (Segment 2)
3.1.5.1.6.6 SWIM shall provide an EBP guard gateway capability to allow a program specialist to examine the blocked messages and, where appropriate, correct problems in the messages that are unrelated to security (e.g. a

typographic error) in a manner which is secured and segregated from all NAS and EBP processing. (Segment 2)

3.1.5.1.6.7 SWIM shall provide an EBP facility that is configurable for multiple instances and types of guard gateways, some provided by the operator of the EBP facility, some provided by NAS service programs. (Segment 2)

3.1.5.1.6.8 SWIM shall provide EBP XML guard gateway functionality for those application data transfers using XML and its associated schema(s). (Segment 2)

3.1.5.1.7 Time Critical Provisioning

3.1.5.1.7.1 SWIM shall provide an EBP capability to support provisioning of direct local connections for time critical data to be exchanged between entities outside the secured NAS perimeter and internal NAS entities in accordance with FAA policy. (Segment 2)

3.1.5.1.7.2 SWIM shall ensure that EBP time critical provisioning uses guard gateways or their functional equivalent as the first processing element on transitioning the secured NAS boundary. (Segment 2)

3.1.5.1.7.3 SWIM shall ensure that the EBP time critical capability includes intrusion detection and monitoring. (Segment 2)

3.1.5.1.7.4 SWIM shall allow EBP time critical provisioning locations to have their status monitored. (Segment 2)

3.1.5.2 Information Systems Security Support Infrastructure

Information System Security Support Infrastructure provides capabilities for managing keys and supporting access control in the NAS.

3.1.5.2.1 SWIM shall provide an enterprise I&KM capability that supports standards-based identification, authentication, integrity, confidentiality, and non-repudiation controls wherever needed within the NAS. (Segment 2)

3.1.5.2.1 Digital Identities

3.1.5.2.1.1 SWIM shall provide I&KM capabilities that support use of all digital identity credentials approved by policy for entity access to a specific NAS information asset. (Segment 2)

3.1.5.2.1.2 SWIM shall provide I&KM capabilities that support use of Personal Identity Verification (PIV) credentials for authenticating the identities of FAA employees and contractors requesting access to NAS information system assets. (Segment 2)

3.1.5.2.1.3 SWIM shall provide I&KM capabilities that support use of PIV credentials issued by other Federal Agencies /Communities for authenticating identities for access to NAS information system assets. (Segment 2)

3.1.5.2.1.4 SWIM shall provide I&KM capabilities that support use of PIV Interoperable (PIV-I) credentials issued by FAA approved Non- Federal Identity Providers for authenticating identities for access to NAS information system assets. (Segment 2)

3.1.5.2.1.5 SWIM shall provide I&KM capabilities that support use of credentials approved by FAA for authenticating identities for access to NAS information system assets. (Segment 2)

3.1.5.2.2 NAS Non Person Entity (NPE) Digital Identities

SWIM I&KM will support the issuance of and use of NPE digital identity credentials approved by policy for use by a NAS information asset/ System to support authentication, integrity, confidentiality and non-repudiation control needs of the NAS.

3.1.5.2.2.1 SWIM shall provide I&KM capabilities for an authorized NAS system administrator to enroll, register and issue NPE credentials approved by policy for use in the NAS. (Segment 2)

3.1.5.2.2.2 SWIM shall provide I&KM capabilities that provide NAS NPE Credential management in accordance with Federal Identity Credentialing and Access Management (FICAM) guidance and FAA Policy. (Segment 2)

3.1.5.2.3 Credential Validation Services

SWIM I&KM will provide digital identity credential validation services for digital identity credentials approved by policy for use by a NAS information asset/ System to support authentication, digital signature, and encryption/decryption needs of the NAS.

3.1.5.2.3.1 SWIM shall provide I&KM capabilities for NAS internal credential validation services in accordance with FAA Policy. (Segment 2)

3.1.5.2.3.2 SWIM shall provide I&KM capabilities for external credential validation services in accordance with FAA Policy. (Segment 2)

3.1.5.2.4 Authoritative Identity Sources

3.1.5.2.4.1 SWIM shall provide I&KM capabilities to utilize centrally managed and maintained directory services (meta and/or virtual directories) of user/entity identity attributes for FAA employees and contractor personnel derived from authoritative sources who have a role based need to access NAS information. (Segment 2)

3.1.5.2.4.2 SWIM shall provide I&KM capabilities to utilize centrally managed and maintained directory services (meta and/or virtual directories) of Non person Entity attributes derived from authoritative sources. (Segment 2)

3.1.5.2.5 Audit & Alerting Capabilities

I&KM will audit transactions and detect component changes in operational status that degrade I&KM services and alert necessary parties to rectify.

3.1.5.2.5.1 SWIM shall provide I&KM capabilities to audit Digital Identity credential creation actions. (Segment 2)

3.1.5.2.5.2 SWIM shall provide I&KM capabilities to audit Digital Identity credential modification actions. (Segment 2)

3.1.5.2.5.3 SWIM shall provide I&KM capabilities to audit Digital Identity credential suspension actions. (Segment 2)

3.1.5.2.5.4 SWIM shall provide I&KM capabilities to audit Digital Identity credential revocation actions. (Segment 2)

3.1.5.2.5.5 SWIM shall provide I&KM capabilities to audit Digital Identity credential validation actions. (Segment 2)

3.1.5.3 SOA Support Platforms

SOA Support Platforms provide an execution environment for operating systems including a Virtual Machine, common language runtime API, and runtime class library for application and Web Services (Java, Microsoft .Net, etc.).

3.1.5.3.1 SWIM shall provide a SWIM services .NET SOA platform. (Segment 2)
3.1.5.3.2 SWIM shall provide a SWIM services JAVA SOA platform. (Segment 2)

3.1.5.4 Web Application Hosting Capability

Web Application Hosting Capability provides hosting functions and platforms that can be used to deploy Interaction Services.

3.1.5.4.1 SWIM shall provide a web application hosting platform. (Segment 2)
3.1.5.4.2 SWIM shall provide a Web Services Framework. (Segment 2)

3.1.5.5 Data Storage

Data Storage primarily considered as the secondary storage for computer files and relational database.

3.1.5.5.1 SWIM shall provide data storage necessary to support SWIM design-time activities. (Segment 2)
3.1.5.5.2 SWIM shall provide data storage necessary to support SWIM run-time activities. (Segment 2)

3.1.5.6 Computing Platform

Computing Platform includes a computer's architecture, operating system, programming languages and related runtime libraries or graphic user interface.

3.1.5.6.1 SWIM shall provide a computing platform necessary to support SWIM design-time activities. (Segment 2)
3.1.5.6.2 SWIM shall provide a computing platform necessary to support SWIM run-time activities. (Segment 2)

3.1.5.7 Terrestrial Network Communication

Terrestrial Network Communication includes the NAS IP network primarily used for data communication between NAS applications, web servers, computer platforms and data storage. (Note: It is expected that SWIM will utilize FTI services to implement the requirements in this section.)

3.1.5.7.1 SWIM shall provide network address lookup functions (e.g., DNS) to allow system end points to be located by user systems within the NAS. (Segment 2)
3.1.5.7.2 SWIM shall provide network address lookup functions (e.g., DNS) to allow service end points to be located by user systems external to the NAS. (Segment 2)

3.1.5.8 Air/Ground Communications - Reserved

3.1.5.9 Sensor Systems - Reserved

3.1.6 Enterprise Governance

3.1.6.1 SOA Runtime Management

3.1.6.1.1 Service Choreography - Reserved

3.1.6.1.2 Service Orchestration

Service Orchestration establishes service interaction patterns for combined, centrally managed services. Orchestration provides mechanisms to coordinate service execution including workflow and business process management.

3.1.6.1.2.1 SWIM shall provide a mechanism to define business rules governing workflow and conditional message routing. (Segment 2)

3.1.6.1.2.2 SWIM shall provide a mechanism to store business rules. (Segment 2)

3.1.6.1.2.3 SWIM shall provide a mechanism to manage business rules. (Segment 2)

3.1.6.1.2.4 SWIM shall provide a mechanism to execute business rules. (Segment 2)

3.1.6.1.2.5 SWIM shall include a mechanism to compose a service from other services. (Segment 2)

3.1.6.1.3 Security Policy Management - Reserved

3.1.6.1.4 Service Policy Management

Service Policy Management is storing, updating, and distributing policies to monitor and control services for faults and performance.

3.1.6.1.4.1 SWIM shall provide a capability to store established service policies. (Segment 2)
3.1.6.1.4.2 SWIM shall provide a capability to query established service policies. (Segment 2)
3.1.6.1.4.3 SWIM shall provide a capability to update established service policies. (Segment 2)
3.1.6.1.4.4 SWIM shall provide a capability to delete established service policies. (Segment 2)
3.1.6.1.4.5 SWIM shall provide a capability to distribute service policy information. (Segment 2)
3.1.6.1.4.6 SWIM shall monitor service policy compliance at run-time. (Segment 2)
3.1.6.1.4.7 SWIM shall provide alerts of service policy non-compliance . (Segment 2)

3.1.6.1.5 Service SLA Management

Services SLA Management is storing, updating, and distributing SLA to control monitoring of faults and quality of services.
SWIM shall audit SLA consumer compliance. (Segment 2)

3.1.6.1.5.1 SWIM shall audit SLA compliance. (Segment 2)
3.1.6.1.5.2 SWIM shall provide a capability to store SLAs. (Segment 2)
3.1.6.1.5.3 SWIM shall provide a capability to query SLAs. (Segment 2)
3.1.6.1.5.4 SWIM shall provide a capability to update SLAs. (Segment 2)
3.1.6.1.5.5 SWIM shall provide a capability to delete SLAs. (Segment 2)
3.1.6.1.5.6 SWIM shall provide a capability to distribute SLAs. (Segment 2)

3.1.6.1.6 Service Scorecard Generation and Publication

Service Scorecard Generation and Publication collects information from Service Enforcement Points to review performance, capacity, reliability and availability of NAS systems and services and validate Service Policy and SLA are fulfilled.

3.1.6.1.6.1 SWIM shall provide service scorecard generation and publication for SWIM services.
3.1.6.1.6.2 SWIM shall include service performance in service scorecards. (Segment 2)
3.1.6.1.6.3 SWIM shall include service capacity in service scorecards. (Segment 2)
3.1.6.1.6.4 SWIM shall include service reliability in service scorecards. (Segment 2)
3.1.6.1.6.5 SWIM shall include service availability in service scorecards. (Segment 2)
3.1.6.1.6.6 SWIM shall include SLA compliance in service scorecards. (Segment 2)
3.1.6.1.6.7 SWIM shall include policy enforcement metrics in service scorecards. (Segment 2)

3.1.6.2 SOA Strategic Governance

SWIM is a key contributor to strategic Governance related to enterprise SOA. SWIM will actively participate in ensuring SWIM services are consistent with NextGen goals and are suitable for a SWIM SOA implementation in the context of services portfolio management. SWIM will participate in activities associated with maintaining technology development consistent with business goals. SWIM will also provide a SOA reference architecture.

3.1.6.2.1 Strategic SOA Governance

Strategic SOA Governance includes strategic planning, funding, budgeting, portfolio management, enterprise architecture, and business and technology alignment.

3.1.6.2.1.1 SWIM shall provide SOA Governance capabilities in support of NextGen and other strategic plans. (Segment 2)

3.1.6.2.2 Service Design Governance

Service Design Governance creates and executes governance process including procedures for the design, implementation, test, and run-time management of the NAS SOA Services.

3.1.6.2.2.1 SWIM shall provide a design-time repository for governance policy, standards and process guidelines to assist in defining rules and policies.
3.1.6.2.2.2 SWIM shall maintain a design-time repository for governance policy, standards and process guidelines to assist in defining rules and policies.

3.1.6.2.2.3 SWIM shall provide a governance design-time repository to contain policies which address SWIM Service registration.
3.1.6.2.2.4 SWIM shall provide a governance design-time repository to contain policies which address SWIM Service versioning.
3.1.6.2.2.5 SWIM shall provide a governance design-time repository to contain policies which address SWIM Service ownership.
3.1.6.2.2.6 SWIM shall provide a governance design-time repository to contain policies which address SWIM Service discovery and access.
3.1.6.2.2.7 SWIM shall provide a governance design-time repository to contain policies which address SWIM Deployment of services.
3.1.6.2.2.8 SWIM shall provide a governance design-time repository to contain policies which address SWIM Security for service.
3.1.6.2.2.9 SWIM shall provide a governance design-time repository to contain policies which address SWIM QoS for service.
3.1.6.2.2.10 SWIM shall provide governance over service design processes and procedures. (Segment 2)
3.1.6.2.2.11 SWIM shall provide governance over service implementation processes and procedures. (Segment 2)
3.1.6.2.2.12 SWIM shall provide governance over service testing processes and procedures. (Segment 2)

3.1.6.2.3 Runtime and Operational Governance

Runtime and Operational Governance create and execute governance process including procedures for runtime management and operations.

3.1.6.2.3.1 SWIM shall provide governance over SWIM run-time management processes and procedures. (Segment 2)
3.1.6.2.3.2 SWIM shall provide governance over SWIM operations processes and procedures. (Segment 2)

3.1.6.2.4 SOA Governance Service Desk Support

SOA Governance Service Desk Support provides a single point of contact to meet the needs and satisfy objectives of both SOA implementers and SOA governance management.

3.1.6.2.4.1 SWIM shall provide single point of contact service desk support to support all SOA governance activities. (Segment 2)

3.1.7 Administrative Services

3.1.7.1 Data/Network Support Services

3.1.7.1.1 Database Administration Services - Reserved

3.1.7.1.2 Network Support Services

Network Support Services provides maintenance of computer hardware and software that comprises a computer network, including deployment, configuration, maintenance, and monitoring.

3.1.7.1.2.1 SWIM shall provide Network Support Services for SWIM-maintained hardware and software capabilities. (Segment 2)

3.1.7.1.3 Information System Security Support Management

ISS Support Management manages the Information System Security Support Infrastructure within the Technical Infrastructure Services area.

3.1.7.1.3.1 SWIM shall provide management capabilities for SWIM-maintained information security infrastructure. (Segment 2)

3.1.7.1.4 Incident Detection and Response Services - Reserved

3.1.7.1.5 Business Continuity Management - Reserved

3.1.7.1.6 Help Desk

Help Desk provides a single point of contact to support NAS personnel in the use of NAS services and to resolve reported problems.

3.1.7.1.6.1 SWIM shall provide Help Desk Support for NAS personnel to report and resolve SWIM service related problems. (Segment 2)

3.1.7.2 Services Provisioning Management

3.1.7.2.1 Services Diagnostics

Services Diagnostics collects fault and performance data to perform diagnostics of services in NAS operation.

3.1.7.2.1.1 SWIM shall collect service fault and service performance data. (Segment 2)

3.1.7.2.1.2 SWIM shall interpret service fault and service performance data to identify performance measures out of conformance with acceptable tolerance values. (Segment 2)

3.1.7.2.1.3 SWIM shall provide a capability to store Service Diagnostics data. (Segment 2)

3.1.7.2.1.4 SWIM shall provide a capability to retrieve Service Diagnostics data. (Segment 2)

3.1.7.2.2 Services Development, Integration and Testing

Services Development, Integration and Testing includes operational testing for service qualities including reliability, availability and SLA policies before deployment.

3.1.7.2.2.1 SWIM shall provide service integration and operational testing for service qualities that include reliability, availability and SLA policy compliance. (Segment 2)

3.1.7.2.3 Services Provisioning

Service Provisioning performs deployment, configuration and maintenance in the lifecycle of SOA Core Services

3.1.7.2.3.1 SWIM shall provide provisioning for SOA Core Services and other SWIM-provided services. (Segment 2)

3.1.7.2.4 Certified Software Management

CSM provides a central source of approved software for use in the NAS, including the ability to ensure the integrity of the software.

3.1.7.2.4.1 SWIM shall provide a software repository for NAS COTS software. (Segment 2)

3.1.7.2.4.2 SWIM shall ensure software repository services are available to all NAS components. (Segment 2)

3.1.7.2.4.3 SWIM shall provide integrity and authentication controls for Software residing within a repository in accordance with FAA Order 1370.104. (Segment 2)

3.1.7.2.4.4 SWIM shall allow the transfer of software and its associated signature from the repository to authorized NAS components. (Segment 2)

3.1.7.2.4.5 SWIM shall allow for the verification of the digital signature associated with transferred software. (Segment 2)

3.2 Product Characteristics and Performance Requirements

3.2.1 Reliability, Maintainability and Availability

3.2.1.1 SWIM shall provide reliability, maintainability and availability in accordance with NAS SR-1000, NAS System Requirements Specification.

3.2.1.2 SWIM shall not degrade safety-critical functions, efficiency-critical functions, essential functions, and routine functions, as applicable to each NAS Application.

3.2.1.3 SWIM shall detect system and service failures in accordance with NAS SR-1000, NAS System Requirements Specification. (Segment 2)

3.2.2 Service Levels

3.2.2.1 SWIM shall support users at peak usage levels, where peak usage is defined in users Service Level Agreement.

3.2.2.2 SWIM shall have continuous operational use. (Segment 2)

3.2.3 Capacity

3.2.3.1 SWIM capacities shall not impact on the capacity and performance of NAS Applications.

3.2.3.2 SWIM shall provide system hardware and software capacity with a relative 50-percent or greater reserve at full operating capability and peak usage levels at delivery. (Segment 2)

3.2.3.3 SWIM hardware and software resources shall be sufficiently scalable to support increased workloads by adding equivalent resources. (Segment 2)

3.2.4 Recovery

3.2.4.1 SWIM shall recover after loss of power within the timeframe specified in accordance with NAS SR-1000 or service level agreement between users.
3.2.4.2 SWIM shall provide diversity across multiple physical locations which provide backup and optionally load balancing capabilities to one another. (Segment 2)
3.2.4.3 SWIM shall provide failure recovery capabilities that allow continued operation in the event of failure of individual SWIM components, or loss or destruction of an entire facility at which SWIM components are located. (Segment 2)
3.2.4.4 SWIM shall provide failure recovery mechanisms that work with existing end-system operations. (Segment 2)
3.2.4.5 Each SWIM physical location shall provide status and administration information sufficient to form a single consolidated view of all NAS boundary operations. (Segment 2)

3.2.5 Performance

3.2.5.1 SWIM shall provide hardware and software performance levels consistent with achieving NAS functional performance requirements specified in NAS SR-1000, NAS System Requirements Specification. (Segment 2)
3.2.5.2 SWIM shall process and use Coordinated Universal Time (UTC) for internal and external time synchronization. (Segment 2)

3.2.6 Operational Software

3.2.6.1 SWIM operational software shall be portable between industry standard operating systems. (Segment 2)
3.2.6.2 SWIM operational software shall be portable between industry standard hardware platforms. (Segment 2)

4.0 Physical Integration

4.1 General

Requirements herein apply to the SWIM Support Infrastructure.

4.1.1 Physical integration shall be in accordance with the physical integration requirements of the implementing programs.

4.2 Real Property

4.2.1 Land

Land procurement/lease is not applicable for the SWIM program.

4.2.2 Space

4.2.2.1 Space for SIP-owned hardware shall be accommodated by implementing programs.
4.2.2.2 Space for SWIM-owned hardware shall be accommodated by the SWIM program office. (Segment 2)

4.3 Reserved

4.4 Environmental

4.4.1 SWIM shall comply with Executive Order (EO) 12873, Federal Acquisition, Recycling, and Waste Prevention.

4.4.2 SWIM and its installations shall comply with FAA Order 1050.1, Policies and Procedures for Considering Environmental Impacts; The National Environments Policy Act (NEPA) of 1969; FAA Order 1050.10, Prevention, Control, and Abatement of Environmental Pollution at FAA Facilities; and 40 CFR, Protection of the Environment.

4.5 Energy Conservation

4.5.1 SWIM shall support NAS facility compliance with:

a) The National Energy Conservation Policy Act.
b) FAA Order 1053.1A, Energy and Water Management Program for FAA Buildings and Facilities,
c) 10 CFR Part 435, Energy Efficiency in Buildings,
d) FAA-HDBK-001, Design Handbook Energy Efficiency and Water Conservation in NAS Facilities, and
e) Executive Order 13123, Greening of Government through Efficient Energy Management.

4.6 Heating, Ventilation, Air Conditioning

4.6.1 SWIM shall support NAS facility compliance with:

a) FAA Order 6970.3-chg37, Plant Equipment Modification–Temperature Control, Ventilation;
b) ASHRAE 55-1992, Thermal Environmental Conditions for Human Occupancy; and
c) ASHRAE 62-2001, Ventilation for Acceptable Indoor Air Quality.

4.7 Grounding, Bonding, Shielding, and Lighting Protection

4.7.1 SWIM installations shall be in accordance with FAA-STD-019, Lightning Protection, Grounding, Bonding, and Shielding for Facilities;

4.7.2 SWIM installations shall comply with applicable sections of the American National Standards Institute (ANSI)/Institute of Electrical and Electronics Engineers (IEEE) 1100-1992,

4.7.3 SWIM installations shall be in accordance with Powering and Grounding Sensitive Electronic Equipment; NFPA Standard 70, National Electric Code and local codes.-

4.8 Cables

4.8.1 SWIM cable installation plans and installation in NAS facilities shall be in accordance with:

a) FAA-G-2100, Section 3.3.1.3.10.2, Electronic Equipment, General Requirements.
b) NFPA 70, National Electrical Code.
c) IEEE STD 1100-1999, Recommended Practice for Powering and Grounding for Sensitive Electric Equipment.

4.9 Hazardous Materials

4.9.1 Handling of hazardous materials shall be in accordance with the 29 Code of Federal Regulations (CFR Title 29, Part 1910), Occupational Safety and Health Standards; FAA Order 8040.4, Safety Risk Management; 29 CFR 1910.1000, Air Contaminants; and 40 CFR 260 to 40 CFR 270 and 40 CFR 700 to 40 CFR 766.

4.9.2 Hazardous materials inherent in SWIM's technology shall comply with FAA Order 1050.1, Policies and Procedures for Considering Environmental Impacts, and FAA Order 1050.10, Prevention, Control and Abatement of Environmental Pollution at FAA Facilities".

4.9.3 SWIM system components shall comply with FAA Order 1050.20, Airway Facilities Asbestos Control; FAA Order 1050.14, Polychlorinated Biphenyls (PCBs) in the National Airspace System (NAS);and 40 CFR Part 82.

4.10 Power Systems and Commercial Power

4.10.1 SWIM power systems and commercial power usage shall comply with applicable sections of FAA-G-2100, Electronic Equipment, General Requirement, and NFPA 70, National Electrical Code.

4.10.2 SWIM power profile characteristics shall comply with applicable sections of FAA-G-2100, Electronic Equipment, General Requirements.

4.11 Telecommunications

4.11.1 SWIM telecommunications requirements shall be in accordance with FAA-STD-029, Selection and Implementation of Telecommunications Standards

4.11.2

4.11.3 SWIM telecommunications requirements shall be in accordance with FAA Order 4441.16, Acquisition of Telecommunications Systems, Equipment and Services;

4.11.4 SWIM telecommunications requirements shall be in accordance with FAA Order 6000.22A-chg3, Maintenance of Analog Lines;

4.11.5 SWIM telecommunications requirements shall be in accordance with FAA Order 6000.47, Maintenance of Digital Transmission Channels; and

4.11.6 SWIM telecommunications requirements shall be in accordance with FAA Order 6000.36A, Communications Diversity.

4.12 Special Considerations

None.

5.0 Functional Integration

5.1 Integration with Other FAA Enterprise Architecture Elements

5.1.1 SWIM shall integrate with existing (legacy) NAS systems.
5.1.2 SWIM shall integrate with NAS systems under development.
5.1.3 SWIM ICDs shall be developed in accordance with FAA Standard 025, Preparation of Interface Control Documents
5.1.4 SWIM shall not degrade the capacities of NAS services.
5.1.5 SWIM shall not degrade the functional capabilities of NAS services.
5.1.6 SWIM shall not degrade the performance of NAS services.
5.1.7 The SWIM interfaces shall accommodate implementation of new NAS systems
5.1.8 The SWIM interfaces shall accommodate in-service transition of NAS systems.
5.1.9 SWIM shall exchange status information with interfacing NAS systems
5.1.10 SWIM installation shall not adversely affect the operation of NAS elements.
5.1.11 SWIM testing shall not adversely affect the operation of NAS elements.
5.1.12 SWIM operation shall not adversely affect the operation of NAS elements.

5.2 Information Requirements

SWIM information requirements are specified in Section 3 of this document.

5.3 Software Integration

5.3.1 SWIM software integration shall not adversely affect the performance of other systems.
5.3.2 SWIM software shall interoperate and communicate in a heterogeneous platform environment.
5.3.3 SWIM software shall be modular, with subsystem and component independence.

5.4 Spectrum Management

Not applicable.

5.5 Standardization

5.5.1 SWIM shall use industry standard operating systems, communication protocols, data management, security, and software languages to ensure interoperability, portability, and maintainability.
5.5.2 SWIM data shall be in accordance with FAA-STD-060, Data Standard for the National Airspace System (NAS).
5.5.3 SWIM hardware and software shall enable the exchange of standardized data elements with automation systems.
5.5.4 SWIM data management shall be in accordance with FAA Order 1375.1, Data Management
5.5.5 SWIM-specific software shall be developed in accordance with FAA-STD-026, Software Development for The National Airspace System (NAS).

5.5.6 Software developed by the implementing programs shall be in accordance with those programs' established software development process. (Segment 1 Only)

5.5.7 SWIM data shall be in accordance with FAA-STD-063 XML Namespaces for the National Airspace System (NAS). (Segment 2)

5.5.8 SWIM information data service registration shall be in accordance with FAA-STD-064 Service Registration for the National Airspace System (NAS). (Segment 2)

5.5.9 SWIM data/information services shall be in accordance with FAA-STD-065 Web Service Specification for the National Airspace System (NAS). (Segment 2)

6.0 Human Integration

6.1 Human Product Interface and Tasks

6.1.1 The SWIM interface shall focus on human-centered design.

6.1.2 SWIM shall consider human system integration during evaluation for selection of SWIM software and hardware.

6.1.3 SWIM shall adhere to the methods, tools, and techniques that ensure products are designed and appropriate for the human workforce that will operate, maintain, and support them in accordance with FAA Order 9550.8.

6.1.4 SWIM shall train integrators in the SWIM human system integration best practice methods, tools, and techniques. (Segment 2)

6.2 Employee Safety and Health

6.2.1 SWIM shall comply with FAA (2003), Human Factors Acquisition Job Aid. (Segment 2)

6.2.2 SWIM shall comply with FAA (2005), Human Factors Design Standard (HFDS). Atlantic City International Airport, FAA William J. Hughes Technical Center. (Segment 2)

6.2.3 SWIM shall comply with Hewitt, G. and R. Gray (2005). Preliminary Human Factors Assessment (HFA) for SWIM JRC. (Segment 2)

6.2.4 SWIM shall comply with Mejdal, S., M. E. McCauley, et al. (2001). Human Factors Design Guidelines for Multifunction Displays, FAA Office of Aerospace Medicine, Civil Aerospace Medical Institute. (Segment 2)

6.2.5 SWIM shall comply with 29USC 794D, The Rehabilitation Act Amendments (Section 508). (Segment 2)

6.2.6 SWIM shall comply with FAA Order 3900.19, Occupational Safety and Health, CFR Title 29 Part 1910.

6.2.7 SWIM shall comply with CFR Title 29 CFR 1910.95 (Code of Federal Regulations), Occupational Safety and Health Standards.

6.2.8 SWIM shall comply with FED-STD-795, Uniform Federal Accessibility Standard (UFAS), April 1988.

6.2.9 SWIM shall comply with Executive Order (EO) 12902, Efficiency and Conservation at Federal Facilities, 8 March 1994.

6.2.10 SWIM shall comply with Occupational Safety and Health Hazards, and with Special Fire Life Safety Requirements, IAW 29 CFR 1960.20.

6.2.11 SWIM shall comply with National Fire Protection Association (NFPA) Standard 70, 1) Clearance Requirements and 2) National Electrical Code.

7.0 Security

This section focuses on requirements for securing the SWIM system information and infrastructure.

7.1 General requirements

7.1.1 The SWIM Architecture shall adhere to NAS Enterprise Information System Security Architecture.

7.1.2 SWIM security policies shall comply with the 44 U.S.C Federal Information System Security Act.

7.1.3 SWIM security policies shall comply with FAA Order 1370.82A, dated September 2006, Information System Security Policy.

7.2 Physical Security

7.2.1 Physical Security Monitoring

7.2.1.1 SWIM shall monitor the physical integrity of SWIM assets, to the maximum extent possible.

7.3 Information Systems Security

7.3.1 System Integrity

7.3.1.1 SWIM shall perform a self –check of security functions at start-up.

7.3.1.2 SWIM shall implement system integrity and protect applicable assets in accordance with NAS-SR-1000, section 3.10.3.5

7.3.2 Availability

7.3.2.1 SWIM shall protect assets from denial of service

7.3.2.2 SWIM shall implement availability and protect applicable assets in accordance with NAS-SR-1000 section 3.10.3.6

7.3.3 Access Control

7.3.3.1 SWIM shall enforce system security rules on an entity's access attempts, in accordance with NAS-SR-1000, section 3.10.3.6

7.3.3.2 SWIM shall enforce separation of security domains.

7.3.3.3 SWIM shall enforce secure import and export of authorized information outside its security domain.

7.3.4 Identification and Authentication

7.3.4.1 SWIM shall uniquely identify all authorized entities
7.3.4.2 SWIM shall authenticate an authorized entity's identity, in accordance with NAS-SR-1000, section 3.10.3.

7.3.5 Confidentially

7.3.5.1 SWIM shall restrict the release of NAS data to authorized users and implement confidentiality/assess clearance in accordance with NAS-SR-1000, section 3.10.3.4.

7.3.6 Non-Repudiation

7.3.6.1 SWIM shall implement non-repudiation, in accordance with NAS-SR-1000, section 3.10.3.7.

7.3.7 Malicious Activity

7.3.7.1 SWIM shall detect malicious activity, in accordance with NAS-SR-1000, section 3.10.3.7.

7.3.8 Security Operations

7.3.8.1 SWIM shall protect access to assets during all operational states, in accordance with NAS-SR-1000, section 3.10.3.8.

7.3.9 Recovery

7.3.9.1 SWIM shall ensure that access control information is recovered after a system failure.
7.3.9.2 SWIM shall ensure that all security functions either complete successfully or recover to a consistent and secure state.

7.3.10Security Management

7.3.10.1 SWIM shall implement technical security management.

7.3.11 Security Audit

7.3.11.1 SWIM shall maintain and record all system access attempts in a security audit log, in accordance with NAS-SR-1000, section 3.10.3.9.

7.4 Personnel Security

7.4.1 SWIM shall comply with FAA Order 1600.1, Personnel Security Program.

8.0 In-Service Support

SWIM capabilities are deployed to NAS operational facilities.

8.1.1 SWIM shall use FAA approved operations and maintenance strategies,
8.1.2 There shall be no SWIM Core Capabilities hardware deployed to operational NAS facilities in Segment 1,

8.1.3 SWIM lab facilities currently at the WJHTC shall be modified to include a SWIM Test Facility as well as a SWIM Support Lab.

8.2 Staffing

8.2.1 SWIM support staffing shall be in accordance with staffing plans put into place by the SWIM implementing programs. (Segment 1 only)

8.2.2 SWIM support staffing shall be in accordance with staffing plans put into place by the SWIM program. (Segment 2)

8.2.3 The operation and maintenance of the SWIM system shall not increase staffing requirements over and above the present NAS staffing at sites, second level engineering activities and the depot.

8.3 Supply Support

8.3.1 SWIM logistics support shall be in accordance with the Integrated Logistics Support Plans established by the implementing programs. (Segment 1 only)

8.3.2 SWIM logistics support shall be in accordance with the Integrated Logistics Support Plan established by the SWIM program. (Segment 2)

8.3.3 SWIM shall be delivered with adequate levels of initial site spares required to facilitate repair and restoration as determined by the implementing programs. (Segment 1 only)

8.3.4 SWIM shall be delivered with adequate levels of initial site spares required to facilitate repair and restoration as determined by the SWIM Program. (Segment 2)

8.4 Support Equipment

8.4.1 Tools and equipment required for SWIM operation and maintenance shall be provided in accordance with the SWIM implementing programs current support equipment strategies. (Segment 1 only)

8.4.2 Tools and equipment required for SWIM operation and maintenance shall be determined by the SWIM program office. (Segment 2)

8.4.3 The maintenance of the system at the site and depot levels shall not require the use of specialized support and test equipment and tools.

8.5 Technical Data

8.5.1 Technical Instruction Books (TIBs), if required, shall be approved and baselined through the SWIM CM process prior to SWIM delivery to the field, for any SWIM Core Capabilities products provided to the SWIM implementing programs. (Segment 1 only)

8.5.2 TIBs, if required, shall be approved and baselined through the SWIM CM process prior to delivery to the field. (Segment 2)

8.5.3 TIBs shall be approved and baselined through the SWIM implementing programs CM process as needed. (Segment 1 only)

8.5.4 TIBs shall be approved and baselined through the SWIM program CM process as needed. (Segment 2)

8.5.5 Second level hardware and software maintenance documentation shall be delivered to the FAA operational support organization prior to SWIM deployment for any SWIM implementing program that uses FAA staff to maintain the hardware or software. (Segment 1 only)

8.5.6 Second level SWIM hardware and software maintenance documentation shall be delivered to the FAA operational support organization staff prior to system deployment. (Segment 2)

8.6 Training and Training Support

8.6.1 System Training

8.6.1.1 Formal training shall be provided for the system through an operational training capability prior to deployment, provided by each implementing program. (Segment 1 only)

8.6.1.2 Formal training shall be provided by the SWIM program prior to system deployment. (Segment 2)

8.6.2 Maintenance Training

8.6.2.1 SWIM training shall provide FAA personnel with the required knowledge and skills required to operate and maintain hardware that is deployed by the implementing programs, in accordance with the implementing programs' training plans. (Segment 1 only)

8.6.2.2 SWIM training shall provide FAA personnel with the required knowledge and skills required to operate and maintain hardware that is deployed, in accordance with SWIM Program training plans. (Segment 2)

8.6.3 Recurrent Training

8.6.3.1 Technical Operations personnel shall receive recurrent skill training as required for the SWIM capabilities, in accordance with the implementing programs' training plans. (Segment 1 only)

8.6.3.2 Technical Operations personnel shall receive recurrent skill training as required for the SWIM capabilities, in accordance with SWIM Program training plans. (Segment 2)

8.6.4 Second Level Engineering Training

8.6.4.1 Second-level engineering training shall be provided for the SWIM system in accordance with the implementing programs' training plans. (Segment 1 only)

8.6.4.2 Second-level engineering training shall be provided for the SWIM system in accordance with the SWIM Program training plans. (Segment 2)

8.7 First and Second Level Repair

8.7.1 SWIM system equipment shall be maintained in accordance with the maintenance plans established by the implementing programs. (Segment 1 only)

8.7.2 SWIM equipment shall be maintained in accordance with the maintenance plans established by the SWIM Program. (Segment 2)

8.7.3 SWIM Second-Level Engineering Support for hardware and software shall be provided in accordance with the second-level engineering support plans established by the implementing programs. (Segment 1 only)

8.7.4 SWIM Second-Level Engineering Support for hardware and software shall be provided in accordance with the second-level engineering support plans established by the SWIM Program. (Segment 2)

8.7.5 SWIM system on-site maintenance shall be conducted in accordance with FAA Order 6000.15C-chg1, General Maintenance Handbook for Airway Facilities.

9.0 Test and Evaluation

9.1 Critical Operational Issues

The following Critical Operational Issues (COIs) have been identified for SWIM:

a) COI-1: Interoperability: Does SWIM interface and operate effectively with existing systems without degrading performance, and do they accommodate defined (and planned) system interfaces and enhancements?
b) COI-2: Transition and adaptation: Does the SWIM system design, training and documentation allow the NAS to be transitioned, adapted and optimized safely and expeditiously for all sites to which it will be deployed?
c) COI-3: Maintenance: Do SWIM's tools, facilities, processes, training and documentation for first-level maintenance, second-level maintenance, and logistics support, enable maintenance tasks to be performed without interruption to Air Traffic Control (ATC) operations?
d) COI-4: Availability: Does SWIM meet the Reliability, Maintainability, and Availability requirements specified in this document.
e) COI-5: Safety and Security: Does SWIM have security controls to protect information, components, applications, and systems that are consistent with, and an integral part of the NAS ISS Architecture.

9.2 Test and Evaluation Requirements

9.2.1 Test and Evaluation shall be conducted to ensure that the functional performance requirements can be met in an operational environment and to address the COIs defined in Section 9.1.

9.2.2 SWIM requirements shall be tested for compliance during Developmental Testing. Developmental Testing shall be conducted to demonstrate that all technical and performance requirements for system hardware and software specified in the development requirements specification have been met.

9.2.3 Integration Testing of SWIM system components shall be conducted at the FAA William J. Hughes Technical Center, where possible, to verify correct implementation of interfaces with other NAS systems.

9.2.4 Integration Testing shall be performed prior to any SWIM capability being delivered operationally.

9.2.5 Operational Testing shall be conducted to verify that SWIM is operationally effective and operationally suitable for use in the NAS and that the NAS infrastructure is ready to accept the system.

9.2.6 SWIM Testing and Evaluation shall be conducted in accordance with the ATO-P T&E Handbook. (Segment 2)

10.0 Implementation and Transition

10.1 SWIM shall provide each implementing program (ERAM, TFMS, AIM, WMSCR, CIWS, ITWS, terminal) with GFE software packages that provide SWIM-required protocols, messaging, and interface management capabilities. (Segment 1 only)

10.2 The implementing programs shall integrate SWIM-provided software packages that provide SWIM-required protocols, messaging, and interface management capabilities into their respective systems. (Segment 1 only)

10.3 Implementing programs shall use existing NAS platforms to the maximum extent feasible for hosting SWIM software. (Segment 1 only)

10.4 The SWIM software shall be included as part of these implementing systems' planned release upgrades, or for new systems, as part of their acquisition process. (Segment 1 only)

10.5 The implementing programs shall transition to SWIM in accordance with the SWIM Governance Plan. (Segment 2)

10.6 The SWIM program office shall host SWIM service container software. (Segment 2)

10.7 The SWIM program shall transition SWIM-provided software packages that provide SWIM-required protocols, messaging, and interface management capabilities into existing SWIM infrastructure in accordance with the SWIM Governance Plan. (Segment 2)

11.0 Quality Assurance

11.1 Quality Program

The SWIM Quality Assurance Plan (QAP) ensures that the SWIM program processes conform to policies and processes of parent organizations (e.g. Department of Transportation (DOT), the FAA and Office of ATC Communications Services (ATO-W)).

11.1.1 The SWIM quality assurance program shall be in accordance with ISO 9001-200 and FAA-Integrated Capability Maturity Model (iCMM) guidelines and the SWIM Quality Assurance Plan (QAP).

11.2 Implementing Program Capabilities

11.2.1 The SWIM quality assurance program for capabilities deployed by the implementing programs (as defined in Appendix C) shall be in accordance with their respective QAP. (Segment 1 only)

11.3 SWIM Program Quality

11.3.1 The SWIM Program shall assign a SWIM Quality Manager to oversee the SWIM quality assurance program. (Segment 2)

11.3.2 The SWIM Program shall control quality related documentation and data. (Segment 2)

11.3.3 The SWIM Program shall identify root causes related to products, services, processes, or the QA plan. (Segment 2)

11.3.4 The SWIM Program shall record problems and root causes related to products, services, processes, or the QA plan. (Segment 2)

11.3.5 The SWIM Program shall take corrective action to prevent recurrence of quality problems. (Segment 2)

11.3.6 The SWIM Program shall take preventive action to prevent occurrence of quality problems. (Segment 2)

11.3.7 The SWIM Quality Manager shall oversee the effectiveness of processes, plans, and QA plan. (Segment 2)

11.3.8 The SWIM Program shall recommend technical and business quality improvements to the SWIM Quality Manager. (Segment 2)

11.3.9 The SWIM Quality Manager shall conduct internal quality audits. (Segment 2)

11.3.10 The SWIM Quality Manager shall document the results of quality audits in reports to the SWIM Program Manager. (Segment 2)

11.3.11 The SWIM Quality Manager shall provide training on quality assurance to SWIM employees. (Segment 2)

12.0 Configuration Management

12.1 Configuration Management Program

12.1.1 The SWIM CM program shall be in accordance with FAA Order 1800.66, Configuration Management Policy and the SWIM Configuration Management Plan.

12.2 Implementing Program Capabilities

12.2.1 The SWIM configuration management program for capabilities deployed by the implementing programs (as defined in Appendix C) shall be in accordance with their respective Configuration Management Program. (Segment 1 only)

12.3 SWIM Program Configuration Management

12.3.1 The SWIM CM program shall be in accordance with the SWIM Configuration Management Plan. (Segment 2)

13.0 In-Service Management

13.1 Supply Support

13.1.1 SWIM implementing programs shall provide supply support in accordance with their current Integrated Logistics Support Plan (ILSP) and maintenance plans. (Segment 1 only)

13.2 Support Facilities

13.2.1 The implementing programs shall be responsible for any support equipment required for maintenance of the SWIM components. (Segment 1 only)

13.2.2 Each implementing program shall provide support in accordance with their existing plans. (Segment 1 only)

13.2.3 In conjunction with the statement of work, SWIM shall provide manpower with skill sets to support SWIM operations and maintenance. (Segment 2)

13.2.4 SWIM designated personnel shall manage Administrative Services, including but not limited to, network and database administration services, directory, and identity services. (Segment 2)

13.2.5 SWIM computing resources (such as servers) shall be operated by SWIM operations staff. (Segment 2)

13.2.6 SWIM Information Technology (IT) resources shall be operated by IT infrastructure support staff. (Segment 2)

13.2.7 SWIM designated personnel shall provide management capabilities for human interaction services, including clients, portals, and notification services. (Segment 2)

13.2.8 SWIM appointed personnel shall manage support services content data, including NAS Mission Services and NAS sensor data acquisition services and systems. (Segment 2)

13.2.9 SWIM appointed personnel shall manage runtime services, which support SWIM-based SOA services. (Segment 2)

13.2.10 The SWIM Program Office shall identify facility support requirements for SWIM. (Segment 2)

13.2.11 SWIM shall contain support facilities that provide data to its requestor(s). (Segment 2)

13.3 Training

13.3.1 The SWIM implementing programs shall perform training in accordance with their existing Program Training Plans. (Segment 1 only)

13.3.2 The SWIM Program Office shall train their personnel, according to current SWIM policies and procedures. (Segment 2)

13.4 First and Second Level Repair

13.4.1 The SWIM capabilities developed by the implementing programs shall be maintained per the current maintenance strategy of the implementing programs. (Segment 1 only)

13.4.2 SWIM and the underlying network services (i.e. FTI, LAN, etc.), shall be supported by Technical Operations (ATO-W). (Segment 2)

13.4.3 SWIM resources (such as servers) shall be maintained by SWIM operations staff. (Segment 2)

13.4.4 SWIM shall perform maintenance on SWIM hardware and software components. (Segment 2)

13.4.5 The SWIM Program Office shall schedule maintenance on hardware and software components in accordance with the defined Maintenance Program Plan. (Segment 2)

13.4.6 The SWIM Program Office shall manage equipment needed to support and test SWIM-related hardware and software components. (Segment 2)

13.5 Packaging, Handling, Storage, and Transportation (PHS&T)

13.5.1 Production Identification and Marking

13.5.1.1 SWIM COI implementing program contractors shall use commercial marking practices for the purposes of product identification, configuration management, and inventory management to control and identify lowest replaceable units (LRUs), in accordance with existing contracts. (Segment 1 only)

13.5.2 Packaging & Transportation

13.5.2.1 All spares shall be packaged using standard commercial packing as specified in ASTM International D3951-95.

13.5.2.2 SWIM COI implementing program contractors shall transport all spares by the most economical means possible, considering dependability, safety, urgency of need, and traceability. (Segment 1 only)

13.5.2.3 SWIM Program Office shall provide configurable storage space for SWIM equipment and operational hardware and software spares. (Segment 2)

13.5.3 Asset Identification – Bar Coding

13.5.3.1 Items provided to SWIM field sites shall be bar coded in accordance with the guidance provided by NAS Logistics Property Management Division of the Technical Operations Service Unit, and as incorporated into the SWIM COIs' existing programs. (Segment 1 only)

13.5.3.2 Items provided to SWIM field sites shall be bar coded in accordance with the guidance provided by NAS Logistics Property Management Division of the Technical Operations Service Unit. (Segment 2)

13.5.3.3 The SWIM Program Office shall provide a mechanism to monitor the depletion of materials needed to support operations and maintenance. (Segment 2)

13.5.3.4The SWIM Program Office shall provide a mechanism to determine the capacity of deployed assets. (Segment 2)

13.5.3.5SWIM shall provide identification and acquisition of materials needed to support operations and maintenance, in accordance to SWIM Program Office acquisition policy. (Segment 2)

13.6 Post Implementation Review

13.6.1 A Post Implementation Review (PIR) shall be conducted six months after each SWIM program component is deployed per the guidelines in the SWIM Implementation Strategy and Planning Document.

13.7 Service Monitoring

13.7.1 SWIM shall monitor the quality of service data, including, but not limited to resource utilization, performance metrics and events associated with overloads, faults, and failures between service providers and service consumers. (Segment 2)

13.7.2 SWIM shall monitor services within SWIM to ensure compliance, specified in the Service Level Agreement. (Segment 2)

13.7.3 SWIM shall monitor services within SWIM to determine if system or service faults have occurred. (Segment 2)

13.7.4 SWIM shall provide a mechanism to alert SWIM Operations Staff when system or service faults have occurred. (Segment 2)

13.7.5 SWIM shall contain service policies, which monitor and manage service faults and service performance. (Segment 2)

13.7.6 The SWIM Program Office shall update service policies, for the continual optimization of service performance. (Segment 2)

13.7.7 The SWIM Program Office shall update service policies, for the continual optimization of service performance. (Segment 2)

13.7.8 SWIM shall collect service performance information, including but not limited to, system capacity, system reliability, and system availability. (Segment 2)

13.7.9 SWIM shall provide strategic acquisition planning, including but not limited to, funding, budgeting, portfolio management, enterprise architecture, and business and technology alignment. (Segment 2)

14.0 System Safety Management

14.1 SWIM Safety Program

14.1.1 The SWIM Safety Program shall be in accordance with the latest FAA Safety Management System (SMS) Manual; the FAA Safety Risk Management Guidance for System Acquisitions (SRMGSA), dated November 29, 2006; and FAA Order 8040.4, Safety Risk Management.

14.2 Implementing Program Capabilities

14.2.1 The Safety Program for capabilities deployed by the implementing programs (as defined in Appendix C) shall be in accordance with their respective Safety Program. (Segment 1 only)

14.3 SWIM Program Safety

14.3.1 The SWIM program office shall identify any hazardous items attributable to the implementation of a SWIM service. (Segment 2)

14.3.2 The SWIM Program shall track all hazards identified using the FAA's Hazard Tracking System (HTS). (Segment 2)

14.3.3 The SWIM Program shall define the current risk level without Program implementation, the transitional risks during implementation, and the residual risks after Program implementation and acceptance in accordance with Chapter 4 of the FAA Safety Risk Management Guidance for System Acquisitions. (Segment 2)

14.3.4 The SWIM Program shall mitigate identified hazards in accordance with Chapter 4 of the FAA Safety Risk Management Guidance for System Acquisitions. (Segment 2)

14.3.5 The SWIM Program shall review all identified safety risks in accordance with the SWIM Safety Plan. (Segment 2)

14.3.6 The SWIM Program shall document in a System Safety Assessment Report (SSAR) the status of every identified hazard. (Segment 2)

Appendix A - Mission Need Correlation Matrix

The following traceability matrix maps requirements addressed in this document, by subsection number, to the SWIM Program Mission Shortfall Statement. No trace is provided for subsections that are included as "Reserved."

Mission Shortfall Statement: **FPR Subsection**	Costs to develop, test, deploy and support new interfaces and applications are too high	The NAS is not an agile air traffic system	Data sharing in the NAS is labor-intensive.	Timely access to common data is lacking in the NAS	The underlying tools to support becoming a performance–based organization are currently lacking
3.1.1 Interaction Services					
3.1.1.1 On-Demand NAS Portal	X	X		X	
3.1.1.2 Administrative Portal	X	X		X	
3.1.1.3 Browser - Reserved					
3.1.1.4 Client - Reserved					
3.1.1.5 Weather Notification - Reserved					
3.1.1.6 Flow Constraint Notification - Reserved					
3.1.1.7 Airport Status and Mission Critical Notification - Reserved					
3.1.2 Mission Services - Reserved					
3.1.3 Support Services					
3.1.3.1 Data Access	X	X	X	X	X
3.1.3.2 Data Flow Management	X	X	X	X	
3.1.4 SOA Core Services					
3.1.4.1 Interface Management	X	X	X	X	
3.1.4.2 Messaging Services		X	X	X	
3.1.4.3 SWIM Security Services	X		X		
3.1.4.4 SWIM Enterprise Services Management		X	X	X	X
3.1.4.5 Collaboration Services - Reserved					

FPR Subsection / Mission Shortfall Statement:	Costs to develop, test, deploy and support new interfaces and applications are too high	The NAS is not an agile air traffic system	Data sharing in the NAS is labor-intensive.	Timely access to common data is lacking in the NAS	The underlying tools to support becoming a performance–based organization are currently lacking
3.1.5 Technical Infrastructure Services					
3.1.5.1 Boundary Protection	X	X			
3.1.5.2 Information Systems Security Support Infrastructure	X	X			
3.1.5.3 SOA Support Platforms	X				
3.1.5.4 Web Application Hosting Capability	X	X		X	
3.1.5.5 Data Storage	X			X	X
3.1.5.6 Computing Platform	X	X			
3.1.5.7 Terrestrial Network Communication		X	X	X	
3.1.5.8 Air/Ground Communications – Reserved					
3.1.5.9 Sensor Systems - Reserved					
3.1.6 Enterprise Governance					
3.1.6.1 SOA Runtime Management	X	X	X		X
3.1.6.2 SOA Strategic Governance	X	X			
3.1.7 Administrative Services					
3.1.7.1 Data/Network Support Services	X				
3.1.7.2 Services Provisioning Management	X	X			X

Appendix B – Acronyms

AAR	Adapted Arrival Route
AAR	Airport Acceptance Rate
ADAR	Adapted Departure and Arrival Route
ADR	Adapted Departure Route
AFP	Airspace Flow Program
AIM	Aeronautical Information Management
AIRMET	Airmen's Meteorological Information
AIXM	Aeronautical Information Exchange Model
ANSI	American National Standards Institute
AOC	Airline Operating Center
ARTCC	Air Route Traffic Control Center
ARTS	Automated Radar Terminal System
ATC	Air Traffic Control
ATCAA	Air Traffic Control Assigned Airspace
ATCSCC	Air Traffic Control System Command Center
ATCT	Airport Traffic Control Tower
ATO	Air Traffic Operations
ATO-W	Office of ATC Communications Services
ATM	Air Traffic Management
AWC	Aviation Weather Center
CCB	Configuration Control Board
CFR	Code of Federal Regulations
CIWS	Corridor Integrated Weather System
CM	Configuration Management
CMLS	Contractor Maintenance and Logistics Support
CMS	Common Message Set
CNS	Communications, Navigation and Surveillance
COI	Community of Interest
COI	Critical Operational Issues
CSM	Certified Software Management

DOT	Department of Transportation
DOTS	Dynamic Ocean Track System
DSP	Departure Sequencing Program
DUATS	Direct User Access Terminal System
EBP	Enterprise Boundary Protection
EDCT	Estimated Departure Clearance Times
EO	Executive Order
ERAM	En Route Automation Modernization
ETA	Estimated Time of Arrival
FAA	Federal Aviation Administration
FCA	Flow Constrained Area
FDIO	Flight Data Input Output
F&FM	Flow and Flight Management
FSS	Flight Service Station
GDP	Ground Delay Program
GFE	Government Furnished Equipment
GS	Ground Stop
HADDS	Host Automation Data Distribution System
HFA	Human Factors Assessment
HFDS	Human Factors Design Standard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I&KM	Identity and Key Management
ICD	Interface Control Document
iCMM	FAA-Integrated Capability Maturity Model
IEEE	Institute of Electrical and Electronics Engineers
ILSP	Integrated Logistics Support Plan
ISS	Information System Security

IT	Information Technology
ITWS	Integrated Terminal Weather System
JPDO	Joint Planning and Development Organization
LOA	Letter of Agreement
LRU	Lowest Replaceable Unit
MIT/LL	Massachusetts Institute of Technology/Lincoln Laboratory
MSS	Mission Shortfall Statement
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NASR	National Airspace System Resources
NCP	NAS Change Proposal
NEPA	National Environments Policy Act
NESG	NAS Enterprise Service Gateway
NextGen	Next Generation Air Transportation System
NORAD	North American Aerospace Defense Command
NTML	National Traffic Management Log
OAG	Official Airline Guide
OI	Operational Improvement
PCB	Polychlorinated Biphenyl
PDC	Pre-Departure Clearance
PHS&T	Packaging, Handling, Storage, and Transportation
PIR	Post Implementation Review
PIREP	Pilot Report
QA	Quality Assurance
QAP	Quality Assurance Plan
QoS	Quality of Service

RMA	Reliability, Maintainability, and Availability
RVR	Runway Visual Range
SAMS	Special Use Airspace Management System
SID	Standard Instrument Departure
SIGMET	Significant Meteorological Information
SMS	Safety Management System
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SRMGSA	Safety Risk Management Guidance for System Acquisitions
SMS	Safety Management System
SRMGA	Safety Risk Management Guidance for Acquisitions
STA	Standard Time of Arrival
STAR	Standard Terminal Arrival Route
STARS	Standard Terminal Automated Radar System
STD	Standard Time of Departure
SUA	Special Use Airspace
SWIM	System Wide Information Management
TBD	To Be Determined
TDDS	Terminal Data Distribution System
TDLS	Terminal Data Link System
TFM	Traffic Flow Management
TFMS	Traffic Flow Management System
TIB	Technical Instruction Book
TM	Traffic Management
TMA	Traffic Management Automation
TRACON	Terminal Radar Approach Control
TS	Thunderstorm
UFAS	Uniform Federal Accessibility Standard
URET	User Request Evaluation Tool

WJHTC	William J. Hughes Technical Center
WMSCR	Weather Message Switching Center Replacement
WSDL	Web Services Description Language
XML	Extensible Markup Language

Appendix C - Overview of SWIM Segment 1 COI Capabilities

The following provides a high level overview of capabilities planned to be included in System Wide Information Management (SWIM) Segment 1 by three Communities of Interest (COIs): Flight and Flow Management, Aeronautical Information Management (AIM), and Weather.

C.1.0 Flight and Flow Management COI

The Flight and Flow Management COI is addressing interfaces between the following domains in SWIM Segment 1:

- En Route and TFM
- Terminal and TFM
- En Route and Terminal
- En Route and External Users
- TFM and External Users

C.1.1 En Route and TFM Interface

C.1.1.1 Flight Data Exchange

TFM currently get flight data from En Route via the Host/ATM Data Distribution System (HADDS) Common Message Set (CMS). SWIM ERAM will enable the HADDS/CMS replacement by providing infrastructure and interfaces that support exchange of existing data between HADDS clients, including support for legacy CMS capabilities.

In SWIM Segment 1, ERAM will provide Flight Data Exchange through the following services:

- Flight Information Service
- Surveillance Information Service
- Sector Information Service
- Route Status Information Service
- General Information Service

The Flight Information Service will provide flight data and updates to clients for filed and active flight plans managed within ERAM and amendments for file flight plans by clients.

The Surveillance Information Service will provide a means to subscribe to track updates and deletions from ERAM. The primary operation of the Surveillance Information Service will be to publish tracks and track updates to clients. The service will support a flexible, open subscription format that allows the subscriber to specify content-based criteria for which track objects the subscriber should be sent and which of the two formats should be sent.

The Sector Information Service will provide a means to query or subscribe to facility sectorization assignments and updates within ERAM.

The Route Status Information Service will provide a means to query or subscribe to adapted arrival and departure route status. The adapted routes are Standard Instrument Departures (SID), Standard Terminal Arrival Routes (STAR), Adapted Arrival Routes (AAR), Adapted Departure Routes (ADR) and Adapted Departure and Arrival Routes (ADAR). The primary operation of the Route Status Information Service will be to publish route status updates to clients.

The General Information Service will provide a means to exchange general information/free text remarks with interfacing systems. The General Information Service will be a peer-to-peer service exposed by ERAM at the ARTCC-Level to exchange messages with peer General Information Services exposed by interfacing systems.

C.1.1.2 Execution of Flow Strategies

TFM, through its Collaborative Decision Making (CDM) programs, facilitates development of aircraft reroutes when necessary due to the effects of weather, facility outages, special events, or emergencies in the NAS. Reroute data exchange between TFMS and ERAM will provide TFM/CDM negotiated reroutes for pre-departure flights via flight object amendments. The SWIM reroute interface will automate what is currently a manual process, whereas the EDCT is already provided as part of the CMS interface. These reroutes and EDCTs will utilize the ERAM Flight Data Exchange capabilities described above.

C.1.1.3 Flow Information Publication

As part of SWIM Segment 1, the Traffic Flow Management System (TFMS) will provide a Flow Information Publication service. The TFMS is a repository of flow information that describes current and planned traffic flow constraints in the NAS. TFMS will provide a Flow Information Publication service that provides a means for ERAM and other clients to subscribe to flow information describing several types of traffic flow constraints. These may include the following:

- Flow Constrained Area (FCA)
- Airspace Flow Program (AFP)
- Ground Delay Program (GDP)
- Ground Stops (GSs)

C.1.2 Terminal and TFM Interfaces

C.1.2.1 Terminal Data Distribution

In the SWIM Segment 1, a new SWIM-based Terminal infrastructure is planned to support publication of terminal data to other domains and subscription to other domain data from the terminal environment. A common platform, referred to as the Terminal Data Distribution System (TDDS), will provide an IP-based front end to existing Terminal legacy systems for which no direct interface currently exists. A number of these Terminal systems, such as Terminal Data Link System (TDLS) /Pre-departure Clearance (PDC), are implemented as a passive tap from an existing En Route to Terminal interface to the flight strip printer. They are therefore limited to only those data elements supported by the current flight strip printer interface. The direct interface will

allow for the bi-directional flow of information and make available status event information previously unavailable from the Terminal domain.

In the Terminal domain, multiple systems duplicate data communications and data management functions. Consolidating these functions in a common infrastructure reduces redundancy, facilitates system evolution and allows partitioning of the applications from data management infrastructure, enhancing system extensibility and flexibility. As part of the SWIM Segment 1, TDDS will be deployed to all large TRACONs and major ATCTs, to consolidate data feeds from the following systems:

- Electronic Flight Strip Transfer System (EFSTS)
- Airport Surface Detection Equipment (ASDE-X)
- Runway Visual Range (RVR).

Airport and surface data exchange supports better departure prediction and airport capacity determination by providing the following elements:

C.1.2.2 Electronic Flight Strip Transfer System (EFSTS) Publication
EFSTS will provide clearance delivery and flight progress taxi status information from the terminal domain via TDDS.

C.1.2.3 Airport Surface Detection Equipment (ASDE-X) Publication
ASDE-X will provide surface surveillance from the terminal domain via TDDS.

C.1.2.4 RVR Publication
Initially, RVR data published will be based on data currently being acquired by TFMS systems at Towers, TRACONs, and Centers. However, once the TDDS is established, TDDS will publish RVR data to interested NAS users.

C.1.3 En Route and Terminal Interfaces

C.1.3.1 Flight Data Input/Output
Terminal currently get flight data in flight strip format from En Route via Flight Data Input/Output (FDIO). This legacy En Route flight data interface exchanges data with 600+ Tower/TRACON locations and supports Flight Strip printing and flight data inputs. SWIM will enable the FDIO replacement using the TDDS to exchange data with the following FDIO clients:

- FDIO replacement in the terminal domain
- TDLS/PDC
- EFSTS.

The ERAM flight data exchange with the TDDS will expand the current limited flight strip information to include access to the full flight object data set.

C.1.4 En Route and External User Interfaces
HADDS/CMS currently provides flight data to a number of external parties including NORAD, customs, Department of Homeland Security, Department of Defense,

government labs and FAA analysis programs. SWIM segment 1 will support the transition of these interfaces to a SWIM service based interface.

C.1.5 TFM and External User Interfaces

C.1.5.1 Flow Information Publication

As part of SWIM Segment 1, the TFMS will provide a Flow Information Publication service. The TFMS is a repository of flow information that describes current and planned traffic flow constraints in the NAS. TFMS will provide a Flow Information Publication service that provides a means for ERAM and other clients to subscribe to flow information describing several types of traffic flow constraints. These may include the following:

- Flow Constrained Area (FCA)
- Airspace Flow Program (AFP)
- Ground Delay Program (GDP)
- Ground Stops (GSs).

TFMS currently provides flow data to a number of external parties including airlines via TMI-NET. SWIM segment 1 will support the transition of these TMI-NET interfaces to a SWIM service based interface.

C.2.0 Aeronautical Information Management COI

Implementation of the AIM capabilities will improve the current Special Use Airspace (SUA) process by providing better knowledge of when a SUA is active or inactive, i.e., unsafe or safe for non-military aircraft to enter. This information will decrease the number of unnecessary aircraft reroutes around SUAs, which in turn will decrease flight time, which in turn will decrease aircraft fuel costs and airline passenger delay time. In ERAM Release 1, ERAM is sharing Special Use Airspace schedule data with TFM. In the SWIM segment 1 timeframe, this data will be shared with a larger number of users.

C.2.1 SUA Automated Data Exchange

Currently, manual data entry processes are used for entering shape definitions and initial SUA schedule data into NASR (National Airspace System Resources) database. There is a lengthy lead-time for establishing and validating SUA geometry data. In Segment 1, a standard data entry user interface to accommodate creation of SUA and ATCAA (Air Traffic Control Assigned Areas) shapes will be provided. Also, these will be automatically stored in the NASR and the National ATCAA database, respectively.

NASR will be enabled to export SUA data to SAMS (SUA Airspace Management System) dynamically via the AIXM (Aeronautical Information Exchange Model) standard. This will improve the current process, where SAMS receives SUA data from NASR as files on a CD every 56 days which is manually loaded onto SAMS

Currently, the only electronic distribution of SUA information is a posting to the sua.faa.gov website, and the information on the website is not updated dynamically. There is manual notification of information changes in SAMS to the downstream

systems, and there is duplicate manual data entry of SAMS information into URET and other downstream systems. The new SUA capability will enable SAMS to publish and distribute SUA information dynamically via the AIXM standard. Furthermore, ERAM will exchange SUA data with SAMS using the AIXM standard.

C.3.0 Weather COI

Thunderstorms (or convective weather systems) are the most significant phenomena impacting NAS operational decisions. ATC decisions are affected by convective weather attributes (e.g., hail, wind shear/microbursts, tornadoes, lightning, turbulence, icing, and reduced ceiling/visibility). Convective weather activity limits the usable capacity of the airspace and directly affects TFM flow-control decisions while ATC decisions are affected more indirectly (i.e., pilot requests for alternate routing or altitude). In the latter case, ATC advises the pilot on avoidance of aviation-impact weather when requested.

Pilot decisions affected by weather range from the highly tactical (escape/impact weather deviations) to the strategic (Route/Altitude selection or Go/No Go that are a part of flight planning). The effects of convective weather are highly dependent on a number of factors including aircraft type, pilot experience, and the airspace where it is encountered. As a result, use and importance of the same weather information can differ from pilot to pilot. Convective weather activity affects all pilot decisions, particularly as it can be unanticipated or develop or move faster/slower than forecast, thereby affecting escape decisions, in-flight route changes, approach commencement, and landing decisions. Forecast activity along an intended flight path, or at the destination airport affects flight planning as well.

Airline dispatchers are located in the Airline Operating Centers (AOCs) (either carrier or third-party vendor) and provide planning and flight monitoring services for assigned aircraft. Their decisions, which range from Go/No Go, in-flight route changes, and route/altitude selection, or diversions, can all be affected by convective weather systems and their attributes. A thunderstorm right over an airport will affect Go/No Go decisions for both arrivals and departures until the activity has passed well out of the area. In-flight route changes are affected as well when convective activity is present in major routing corridors or jetways and routes en route to or at destination terminals.

C.3.1 PIREP Data Publication

One of the SWIM Segment 1 capabilities being developed by the Weather COI is the ability to automatically distribute Pilot Reports (PIREPs) to en route controllers. ERAM will provide controllers with an interface to convert voice PIREPs into auto-PIREPs, and will send the auto-PIREPs to the Weather Message Switching Center Replacement (WMSCR) System. WMSCR will redistribute these via SWIM services to the wider NAS community and to weather forecasts at all levels. Since approximately 90% of PIREPs ‘fall on the floor,’ distribution of these crucial observations via WMSCR will enhance safety and capacity.

C.3.2 Integrated Terminal Weather System (ITWS) Publication

The SWIM ITWS Publication will provide ITWS products to the Airline Operational Centers (AOCs), to the National Weather Service (NWS) and to pilots. Sharing of

ITWS products with all NAS users promotes common situational awareness, which is absolutely crucial to the collaborative decision making (CDM) process that is necessary to reduce weather-related delays.

Greater distribution of ITWS data products will enhance NAS capacity by improving efficiency, as it displays convective weather and associated attributes at selected NAS pacing airports to traffic managers and dispatchers. ITWS also provides a real-time picture of aviation-impacting weather to traffic managers at ARTCCs, the ATCSCC, and large TRACONs via the ITWS Situation Display (SD). This enables Traffic Managers and controllers to track storm activity at major NAS airports, to comprehend airport acceptance rates (AAR), and to facilitate the traffic flow movement to mitigate the effect of weather on NAS operations.

With its microburst prediction capability, ITWS also increases aircraft safety on runways and in approach/departure corridors at NAS pacing airports by providing controllers [and pilots via Terminal Weather Information for Pilots (TWIP)] with advance notice of the likelihood of a wind shear/microburst event. ITWS capacity enhancements include gust-front prediction that enables controllers to optimize runway usage prior to wind-shift passage to help mitigate decreased Airport Acceptance Rate (AAR). The 1-hour Terminal convective weather forecast enables TRACON controllers to anticipate storm passage near gates so that they can maintain a safe and orderly flow of air traffic.

C.3.3 Corridor Integrated Weather System (CIWS) Publication

The SWIM CIWS Publication will provide CIWS products to the Airline Operational Centers (AOCs), to the National Weather Service (NWS) and to pilots. Greater distribution of CIWS functionality will not only provide the ability for traffic managers to collaborate on weather-avoidance routing/re-routing with dispatchers, but will also help to avoid en route delays, in turn helping to save airline fuel costs.

In the en route domain, CIWS produces an automated two-hour regional convective weather forecast (national forecast by the beginning of SWIM Segment 1), which will be available to traffic managers so they can determine the gaps in the convective weather activity and optimize routing. CIWS also provides current and forecast convective weather echo tops which enables traffic managers to exploit potential over-the-top routing.

Appendix D - Applicable Documents

The following specifications, handbooks, orders, standards, and drawings form a part of the requirements and are applicable to the extent specified herein. The latest version of these documents on the date of this approved document shall apply.

D.1.0 FAA/DOT Specifications, Standards, and Orders

NAS SR-1000	NAS System Requirements Specification.
FAA-HDBK-001	Design Handbook Energy Efficiency and Water Conservation in NAS Facilities
FAA-STD-019	Lightning Protection, Grounding, Bonding, and Shielding for Facilities
FAA-STD-029	Selection and Implementation of Telecommunications Standards
FAA Order 1050.1	Policies and Procedures for Considering Environmental Impacts
FAA Order 1050.10	Prevention, Control, and Abatement of Environmental Pollution at FAA Facilities
FAA Order 1053.1A	Energy and Water Management Program for FAA Buildings and Facilities
FAA Order 1050.14	Polychlorinated Biphenyls (PCBs) in the National Airspace System (NAS)
FAA Order 1050.20	Technical Operations Asbestos Control
FAA Order 1370.104	Digital Signature Policy
FAA Order 1370.82A	Information System Security Policy
FAA Order 1370.94	Wireless Technologies Security Policy
FAA Order 1370.95	Wide Area Network Connectivity Security
FAA Order 1375.1	Data Management
FAA Order 1600.1	Personnel Security Program
FAA Order 1800.66	Configuration Management Policy
FAA Order 3900.19	Occupational Safety and Health
FAA Order 4441.16	Acquisition of Telecommunications Systems, Equipment and Services
FAA Order 6000.15C	General Maintenance Handbook for Technical Operations. -chg1,
FAA Order 6000.22A	Maintenance of Analog Lines -chg3
FAA Order 6000.36A	Communications Diversity.
FAA Order 6000.47	Maintenance of Digital Transmission Channels
FAA Order 6970.3-chg37	Plant Equipment Modification–Temperature Control, Ventilation
FAA Order 8040.4	Safety Risk Management FAA Safety Risk Management Guidance for System Acquisitions (SRMGSA), dated November 29, 2006
FAA-G-2100	Section 3.3.1.3.10.2, Electronic Equipment, General Requirements

FAA-STD-026	Software Development for The National Airspace System (NAS)
FAA-STD-029	Selection and Implementation of Telecommunications Standards
FAA-STD-060	Data Standard for the National Airspace System (NAS)
	Human Factors Acquisition Job Aid (2003).
	Human Factors Design Standard (HFDS) (2005)
	Preliminary Human Factors Assessment (HFA) for SWIM JRC, Hewitt, G. and R. Gray (2005)
	Human Factors Design Guidelines for Multifunction Displays, FAA Office of Aerospace Medicine, Civil Aerospace Medical Institute, Mejdal, S., M. E. McCauley, et al. (2001).
	Human Factors Design Guide for Acquisition of Commercial-Off-The-Shelf Subsystems, Non-Developmental Items, and Developmental Systems,
	Executive Order (EO) 12902, Efficiency and Conservation at Federal Facilities, 8 March 1994
	FAA Information System Security Architecture Version 5
	SWIM Quality Assurance Plan
	SWIM Configuration Management Plan
	SWIM Implementation Strategy and Planning Document.
	ATO-P Test and Evaluation Handbook, dated August 28, 2008.

D.2.0 Other Publications and Specifications

	The National Energy Conservation Policy Act
	The National Environments Policy Act (NEPA) of 1969
10 CFR Part 435	Energy Efficiency in Buildings
Executive Order 13123	Greening of Government through Efficient Energy Management
Executive Order 12873	Federal Acquisition, Recycling, and Waste Prevention
Executive Order 12902	Efficiency and Conservation at Federal Facilities, 8 March 1994
29 CFR	Code of Federal Regulations (CFR Title 29, Part 1910), Occupational Safety and Health Standards
29 CFR1910.1000	Air Contaminants
29 CFR 1960.20	Occupational Safety and Health Hazards, and with Special Fire Life Safety Requirements
40 CFR 260 to 40 CFR 270	
40 CFR 700 to 40 CFR 766	
40 CFR	Protection of the Environment
40 CFR Part 82	
FAA Order 8040.4	Safety Risk Management;
FED-STD-795	Uniform Federal Accessibility Standard (UFAS), April 1988

Standard 70	National Fire Protection Association (NFPA), 1) Clearance Requirements and 2) National Electrical Code
10 CFR Part 435	Energy Efficiency in Buildings
ASHRAE 55-1992	Thermal Environmental Conditions for Human O Occupancy
ASHRAE 62-2001	Ventilation for Acceptable Indoor Air Quality.
	American National Standards Institute (ANSI)/Institute of Electrical and Electronics Engineers (IEEE) 1100-1992
	ANSI/IEEE STD 1100-1999, Recommended Practice for Powering and Grounding for Sensitive Electric Equipment
	44 U.S.C Federal Information System Security Act
	ISO 9001-200 and *FAA-Integrated Capability Maturity Model* (iCMM)
D3951-95	ASTM International
29USC 794D	The Rehabilitation Act Amendments (Section 508)
HSPD-12	Homeland Security Presidential Directive 12 (HSPD-12): Policy for a Common Identity Standard for Federal Employees and Contractors.
FISMA	Federal Information Security Management Act (FISMA) of 2002
OMB M 04-04	OMB Memorandum M 04-04: E-Authentication Guidance for Federal Agencies.
OMB M 05-05	OMB Memorandum M 05-05: Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services.
NIST 800-53	Recommended Security Controls for Federal Information Systems and Organizations
FIPS PUB 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS PUB 200	Minimum Security Requirements for Federal Information and Information Systems